FACULTAT D'INFORMÀTICA DE BARCELONA (FIB)
UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC)

ARDITEC - ARDICLOUD

Implementación de Microsoft System Center Virtual Machine Manager en entorno *Cloud*

Alberto Illobre

Ingeniería de Computadores

***Director**: José Miguel Aroca*

Arditec Sistemas, S.L

***Ponent**: David López*

Departamento de Arquitectura de Computadores (AC)

Enero de 2019

Agradecimientos

Me gustaría agradecer a todo el equipo de ArdiTec, por la ayuda ofrecida durante la realización del proyecto. En especial a mi director José Miguel Aroca, por haberme dado la oportunidad de participar en él y por guiarme durante todos los pasos seguidos.

Agradecer también el apoyo de mis padres durante todo el transcurso del proyecto, en especial durante las semanas previas al inicio.

Por último, me gustaría agradecer especialmente a Clara, por su paciencia y su ayuda para mantener la calma durante toda la realización del proyecto

Resumen

Debido a las claras ventajas que ofrece el *Cloud* cada vez más empresas se interesan por utilizar este servicio. Gestionar estos entornos sin el soporte de una herramienta implica tener que acceder a los servidores para realizar cualquier tipo de acción sobre estos. Además, el despliegue de máquinas virtuales puede ser un proceso largo, que en muchas ocasiones se puede evitar, o ahorrar gran parte de éste, con la ayuda de plantillas. Estos hechos implican que los entornos *Cloud* requieran de un sistema que facilite el trabajo de gestión.

Por este motivo, durante este proyecto se ha estudiado la herramienta Microsoft System Center Virtual Machine Manager para mejorar dicha gestión. Esta herramienta permite, entre otras cosas, ofrecer un acceso mediante permisos a la gestión de máquinas virtuales. Además, ofrece un sistema de plantillas que permite desplegar una o varias máquinas virtuales con una configuración específica en cuestión de minutos.

Para el desarrollo de este proyecto, se han diferenciado tres fases. En una primera fase, se realiza un estudio de requisitos y una posterior instalación en un entorno de pruebas específicamente preparado para esta tarea. Seguidamente, se han realizado varias pruebas para comprobar el funcionamiento de lo que se ha considerado esencial para la implementación en el entorno *Cloud* real. Por último, se ha planificado la instalación en dicho entorno. Esta herramienta, sin embargo, tiene ciertas funcionalidades que son útiles en entornos mucho mayores y que, por tanto, no se han cubierto en este proyecto.

Tabla de contenido

Introducción y contextualización

1.1 Contexto

Hoy en día una enorme cantidad de información fluye por internet debido a la gran cantidad de usuarios, como muestra la Figura 1.1, no sólo para comunicaciones, sino que también para proveer servicios. Es por esto por lo que la tecnología de *Cloud computing* se ha popularizado mucho en los últimos años.

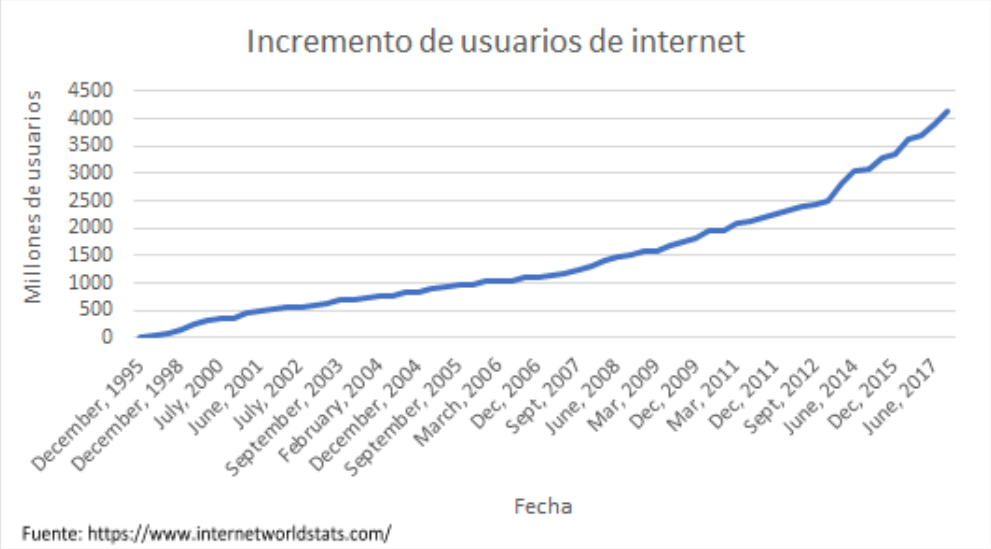


Figura 1.1: Incremento de usuarios de Internet desde 1995.

Se puede describir el término *Cloud* como la entrega de servicios informáticos (servidores, almacenamiento, bases de datos, redes, software, análisis, etc.) a través de Internet (*la nube*).

El *Cloud computing* tiene sus orígenes en los años sesenta cuando comenzaron a asentarse las bases de esta tecnología. En esa época, las empresas empezaron a necesitar consultar grandes cantidades de información desde distintos puntos de acceso. Sin embargo, el coste de las infraestructuras era muy elevado y se iniciaron estudios para encontrar la forma de integrar una CPU con acceso a múltiples usuarios.

Algunos expertos indican que fue John McCarthy[1] quien introdujo este concepto en 1961, autor a quién también se le atribuye el concepto de inteligencia artificial. Otros autores atribuyen el concepto de *Cloud computing* a Joseph Carl Robnett Licklider[2] cuya visión era crear una red de ordenadores mundial para que todo el mundo pudiera tener acceso a programas y datos independientemente de la ubicación.

[1] https://es.wikipedia.org/wiki/John_McCarthy
[2] https://es.wikipedia.org/wiki/Joseph_Carl_Robnett_Licklider

El concepto de computación compartida evolucionó considerablemente a finales de los años 90, cuando la red de Internet contaba con ancho de banda suficiente como para soportar el peso del *Cloud*. En 1999 se produjo un gran hito en *Cloud computing* con la inauguración de Salesforce[1], pionero en la entrega de aplicaciones empresariales a través de una web simple. A partir de ese momento, las grandes empresas de informática (Google, Amazon, Ibm o Microsoft) empezaron a interesarse por los servicios de *Cloud computing* y empezó la innovación y desarrollo de los diferentes tipos de *Cloud*.

Existen tres tipos de *Cloud*; público, privado e híbrido. Un proveedor de *Cloud* público proporciona recursos tanto a particulares como a empresas. Por el contrario, el *Cloud* privado se define como la oferta de servicios para un público específico y muchos de los beneficios de un *Cloud* público, con el añadido de ofrecer mayor seguridad y privacidad. Por último, en el *Cloud* híbrido una parte de los servicios se ofrecen de manera pública, y otros de manera privada.

Para este proyecto, nos hemos centrado en el *Cloud* privado y, por tanto, es necesario saber que modelos de servicio se pueden ofrecer. Existen tres modelos principales de *Cloud computing*: *Infrastructure as a Service (*IaaS), *Platform as a Service* (PaaS) y *Software as a Service (SaaS),* como se muestra en la Figura 1.2. De entre los tres modelos, un *Cloud* privado puede ofrecer dos de ellos: *IaaS* y *PaaS*. El primero permite al proveedor ofrecer recursos de la infraestructura (CPU, memoria, red y almacenamiento) como servicio. Es el proveedor, por tanto, quien se encarga de la complejidad de la infraestructura física y lógica. El segundo permite ofrecer aplicaciones, eliminando la necesidad de administrar la infraestructura (aprovisionamiento de recursos, planificación de la capacidad, mantenimiento del software/hardware).

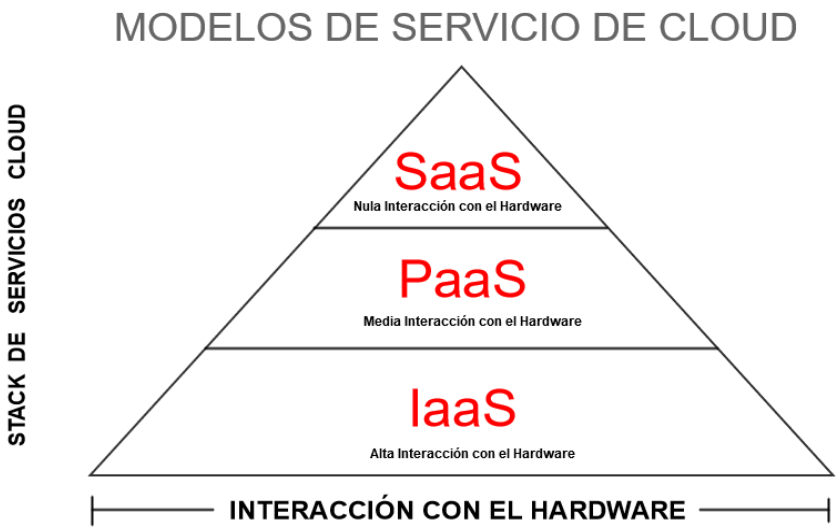


Figura 1.2: Capas del *Cloud computing*[2].

[1] https://www.salesforce.com/es/company/about-us/
[2] Fuente: https://www.hostingred.com/wp-content/uploads/2016/11/*Cloud*2.png

En lo que concierne a los usuarios finales, algunas de las ventajas del *Cloud computing* son:

i. Reducción de costes: el *Cloud computing* permite eliminar la inversión de capital inicial que supone la adquisición de hardware/software de un centro de datos local. Además, el coste de mantenimiento suele ser menor.
ii. Escalabilidad: Permite el aprovisionamiento de recursos en tiempo real, transparente a los usuarios.
iii. Independencia dispositivo-ubicación: permite a los usuarios acceder a los sistemas independientemente de su ubicación y del dispositivo que esté utilizando.
iv. Rendimiento: gracias a la virtualización, se puede aprovechar al máximo los recursos que ofrecen los equipos.
v. Mantenimiento: las aplicaciones que cada usuario necesite no tienen que estar instaladas en cada equipo, sino que se ejecutan desde el *Cloud*.

En cuanto a las desventajas, podemos destacar que la disponibilidad de las aplicaciones es dependiente de la disponibilidad de acceso a Internet.

Los entornos *Cloud* pueden resultar complejos debido a la posibilidad de tener diferentes dispositivos y sistemas trabajando conjuntamente. La gestión de estos entornos puede llegar a ser complicada utilizando únicamente las herramientas estándar. Para solucionarlo existen herramientas que permiten lograr una gestión centralizada de toda la infraestructura lógica/virtual de un *Cloud*. Este proyecto se ha centrado en la implementación de una de estas herramientas, que no sólo simplifica el trabajo de los usuarios encargados de gestionar el sistema, sino que también permite tener un mayor control sobre lo que cada usuario puede hacer.

1.2 Actores

Los sistemas de administración/gestión de entornos de virtualización permiten a los departamentos I.T. (del proveedor de servicios y/o del cliente final) gestionar su entorno *Cloud*. El beneficio principal que se obtiene es la simplificación de las tareas, en ocasiones tediosas cuando hablamos de entornos complejos.

El principal y único actor al que va dirigido este proyecto es el departament IT de ArdiTec ya que será éste quien lo utilice y se beneficie por tanto de su uso. Dichos sistemas permiten, entre otras cosas, la utilización de plantillas para la creación y despliegue de máquinas virtuales (en adelante VMs), la posibilidad de hacer cambios sin acceder a la infraestructura base, aumentar la seguridad de la administración del entorno *Cloud* mediante permisos basados en usuarios/grupos, etc.

1.3 Estado del Arte

Existen diferentes sistemas de virtualización con sus hipervisores o monitores de VMs específicos de gestión. Un hipervisor es una plataforma que permite, mediante la virtualización, alojar y ejecutar distintos sistemas operativos simultáneamente sobre la misma plataforma hardware, de una manera eficaz y sin conflictos. Los hipervisores ofrecen un hardware virtual a los sistemas operativos virtuales (sistemas invitados), y así poder aislar a los sistemas operativos de los recursos hardware reales y controlar el acceso a éstos. Entre los hipervisores existentes, podemos distinguir dos tipos en función de su manera de ejecutarse: tipo 1 y tipo 2.

Los hipervisores de tipo 1 (*nativo, unhosted, bare metal*) se ejecutan sobre el hardware, como muestra la Figura 1.3. Algunos de los hipervisores que podemos encontrar de este tipo son: VMWare[1], Citrix Xen Server[2], Oracle VM Server[3] o Microsoft Hyper-V Server[4]. Los hipervisores de tipo 2 (*hosted)* requieren de un sistema operativo en ejecución, como muestra la Figura 1.4. Algunos ejemplos de hipervisores son: Oracle VirtualBox[5], VMWare Workstation[6], QEMU[7] o Microsoft Virtual PC[8].

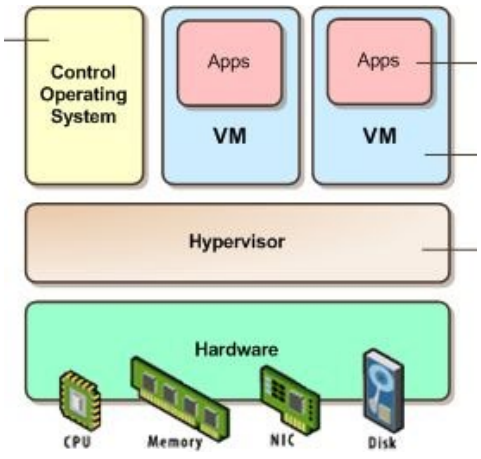


Figura 1.3: Hipervisor tipo 1.

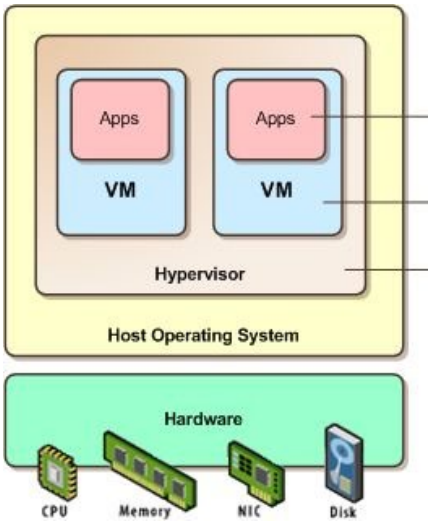


Figura 1.4: Hipervisor tipo 2.

Para este proyecto, nos centraremos en los hipervisores de tipo 1. Como ya se ha mencionado, existen varios hipervisores de este tipo, entre los cuales destacan VMWare y Microsoft Hyper-V Server. Pese a que VMWare haya sido pionero en virtualización y haya sido el que ha obtenido

[1] https://www.vmware.com/
[2] https://www.citrix.es/products/citrix-hypervisor/
[3] https://www.oracle.com/es/virtualization/vm-server-for-x86/index.html
[4] https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/about/
[5] https://www.virtualbox.org/
[6] https://www.vmware.com/es/products/workstation-pro.html
[7] https://www.qemu.org/
[8] https://www.microsoft.com/es-es/download/details.aspx?id=3702

durante muchos años los mejores resultados, el sistema de Microsoft obtuvo una notable mejora en su versión de Hyper-V de 2012 y hoy en día son muy similares, siendo Hyper-V la opción más barata, y por tanto la más utilizada en pequeñas empresas.

Cada sistema de virtualización tiene su propia herramienta de administración de VMs, como vCenter para VMWare, o System Center Virtual Machine Manager para Hyper-V. Puesto que en el entorno real, y por tanto en el de testeo, se está utilizando Microsoft Hyper-V Server, y pese a que la mayoría sean de estas herramientas sean compatibles con otros hipervisores, siempre es recomendable utilizar la herramienta propietaria, puesto que es mucho más especializada y aprovecha mejor los recursos propios del hipervisor. Por este motivo, el sistema escogido *es System Center Virtual Machine Manager* (en adelante *SCVMM)*.

Las características de *VMM* incluyen:

i. Centro de datos: Configuración y gestión de los componentes del centro de datos (hosts de virtualización, redes, recursos de almacenamiento) como un único tejido. *VMM* aprovisiona y administra los recursos necesarios para implementar VMs y servicios en nubes privadas.
ii. Hosts de virtualización: *VMM* puede agregar, aprovisionar y administrar clústeres y hosts de Hyper-V y VMware.
iii. Redes: Con *VMM* se pueden agregar recursos de red al tejido de *VMM,* incluidos sitios de red definidos por subredes IP, VLANs, conmutadores lógicos y virtuales y direcciones IP estáticas. Además, proporciona virtualización de red para permitir aislar las redes para mayor privacidad y seguridad.
iv. Almacenamiento: *VMM* puede detectar, clasificar, aprovisionar y asignar almacenamiento local y remoto.
v. Recursos de biblioteca: El tejido de *VMM* cuenta con una biblioteca de recursos utilizados para crear e implementar VMs y servicios en hosts de virtualización. Se pueden almacenar discos duros virtuales, imágenes ISO, scripts, plantillas y perfiles (utilizados para agilizar la creación de VMs).

La primera versión realmente operativa en entornos de producción del sistema *SCVMM* fue la 2008 R2. Aunque existieron versiones anteriores de *SCVMM*, estas tuvieron un uso aislado debido a la inmadurez del propio hipervisor (Microsoft Hyper-V).

Formulación del problema

El objetivo final del proyecto es la puesta en producción del sistema de Microsoft, *SCVMM,* que se utilizará para mejorar y facilitar las tareas de mantenimiento y gestión de Ardi*Cloud* (servicio *Cloud* de ArdiTec Sistemas). Para lograrlo, hay que pasar por una fase previa de experimentación de la herramienta, para comprobar que cumple con los requisitos esperados y por eso, hay una serie de objetivos para pautar el avance del proyecto.

Objetivo 1: Preparación del entorno físico y virtual del entorno de testeo.
Comprobar las funcionalidades de la herramienta no es algo que se pueda hacer directamente *en caliente* en los servidores donde trabajan los usuarios finales, por tanto, es necesaria una preparación en un laboratorio, basado en un entorno del *Cloud* real.

Cabe destacar que en este objetivo se incluye el estudio previo necesario para la preparación del entorno, es decir, el estudio de requerimientos y/o recomendaciones de Microsoft antes de empezar con la implementación del sistema.

Objetivo 2: Testeo de las funcionalidades de la herramienta *SCVMM*.
Es importante hacer pruebas del uso que se le pretende dar a la herramienta, no sólo para comprobar que realmente cumple con los requisitos esperados, sino que también hay que investigar dónde están los límites en las funcionalidades que ofrece.

Objetivo 3: Puesta en producción y formación a usuarios finales.
El objetivo final es poder poner en producción el sistema y, por tanto, es necesario formar a los usuarios finales para así agilizar su proceso de aprendizaje.

Alcance y obstáculos

3.1 Alcance

Tal y como se ha explicado anteriormente, el objetivo del proyecto es la implementación de *SCVMM* en un entorno actualmente ya en producción. Al ser un sistema que lleva años en el mercado, el proyecto cubre principalmente la parte experimental previa a la puesta en producción del sistema.

3.2 Posibles obstáculos

En caso de querer implementar un sistema de gestión centralizada *SCVMM* en entornos de producción, el obstáculo principal serían los costes: licenciamiento del sistema, requerimientos hardware, etc.

Para este proyecto en cuestión, teniendo en cuenta que partimos de un entorno actualmente en producción, el obstáculo principal es precisamente ese: el hecho de estar en producción. La posible necesidad de modificar la infraestructura (principalmente la de red) para adaptarla a los requerimientos y/o recomendaciones de Microsoft *SCVMM*, supondría un obstáculo no insalvable pero sí importante. Si fuera el caso, debería realizarse un estudio y una planificación exhaustiva sobre qué cambios habría que realizar y cuándo (paradas programadas), y cuál sería la duración de las paradas programadas. En caso de tener que realizar cambios que requieran detener los servicios, también es necesario notificar previamente a los clientes afectados (según los servicios a parar) para evitar cualquier tipo de problema.

Metodología

La metodología seguida durante el desarrollo del proyecto es la metodología en cascada, como se muestra en la Figura 4.1.

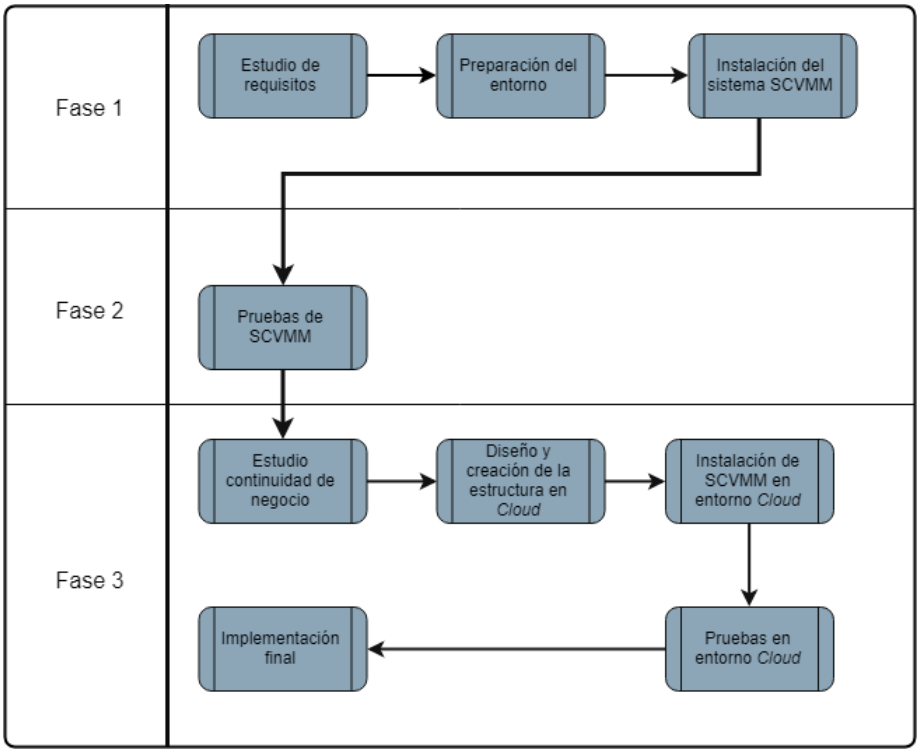


Figura 4.1: Metodología de trabajo.

Al tratarse de un proyecto cuyo objetivo principal es la implementación del sistema (*SCVMM*) y teniendo en cuenta que estamos integrados en el departamento encargado de la gestión de la infraestructura *Cloud*, existirá un seguimiento constante para el avance del proyecto y cada paso será validado.

En una primera fase de testing se ha recreado la infraestructura *Cloud* con los elementos mínimos en número, pero con las mismas funcionalidades. Así pues, tanto en el entorno real como en el de testing disponemos de hosts de virtualización, unidades de almacenamiento compartido SAN, espacios de almacenamiento de red NAS, electrónica de red, etc. El esquema de esta primera fase es el que se muestra en la Figura 4.2.

Para ello se han preparado dos máquinas en dominio que actúan como *hosts de virtualización,* donde se ejecutan las VMs (entre las cuales están las propias del sistema *SCVMM* (servidor *VMM*, base de datos SQL, biblioteca y consola). Se ha habilitado un almacenamiento compartido, al que están conectados ambos hosts mediante *iSCSI*[1], donde se almacenan los archivos de

[1] Internet Small Computer System Interface: protocolo para comunicación de dispositivos a través de la red.

configuración y los discos duros de las VMs. Un tercer host virtual hace únicamente la función de *controlador de dominio*[1] (DC).

Evidentemente el entorno de producción dispone de más y mejores hosts de virtualización, mejores sistemas de almacenamiento, elementos de red… aunque la estructura funcional a grandes rasgos es exactamente la misma.

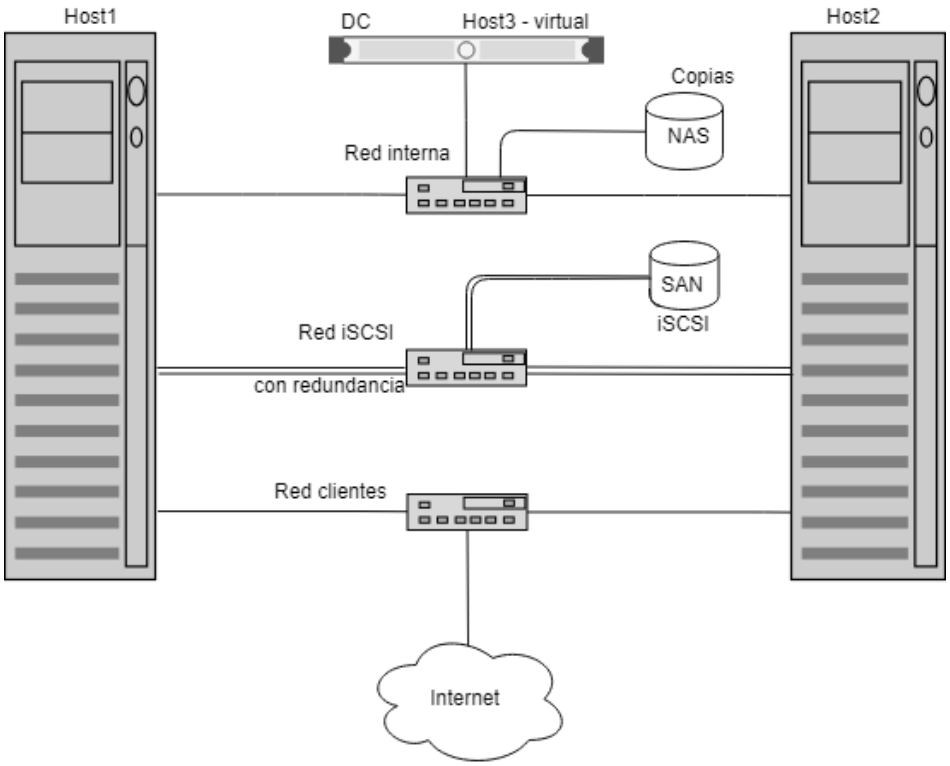


Figura 4.2: Infraestructura del entorno *Cloud* de pruebas.

Una vez esté el entorno preparado, se han realizarán una serie de pruebas para verificar que el sistema cumple con las funcionalidades esperadas. Estas pruebas consistirán en:

i. Pruebas de seguridad vía usuarios/grupos: una de las funcionalidades de *SCVMM* es asignar permisos a usuarios/grupos para administrar ciertos recursos. Supongamos que una organización tiene 3 niveles de seguridad en cuanto a la administración de la infraestructura *Cloud*, siendo, por ejemplo, el nivel 3, el de mayor seguridad. Algunos recursos deberían ser accesibles únicamente por los usuarios que tengan ese nivel para evitar que alguien, ya sea por falta de conocimiento o con malas intenciones, provoque algún error crítico en la infraestructura.

ii. Plantillas de VMs: Otra funcionalidad importante es la capacidad de desplegar VMs a partir de plantillas (almacenadas en repositorios), lo que permite minimizar los tiempos de entrega de dichas VMs. También será necesario comprobar la creación y despliegue de VMs desde 0 (sin utilizar plantillas).

[1] Su función principal es la autenticación: garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña.

iii. Redes virtuales: El uso de redes virtuales nos permite aislar entornos a nivel de red, lo que aumenta la seguridad y la privacidad de la información. Desde *SCVMM* podrán crearse de manera mucho más sencilla.
iv. Pruebas de conmutación por error: se realizarán pruebas de continuidad del servicio ante los fallos habituales en cualquiera de los componentes críticos del sistema.
v. Caída del propio sistema *SCVMM:* Se realizarán pruebas para comprobar qué sucede si el propio sistema cae. Cabe destacar que un fallo del sistema *SCVMM* no implica el fallo de todo el sistema de virtualización, la implicación que tendría sería la necesidad de realizar las tareas de gestión de manera manual, sin la ayuda de *SCVMM*.
vi. Pruebas de recuperación frente a desastres. Tiempo de recuperación ante un desastre.
vii. Sistema de logging/reporting. En estos entornos es imprescindible la respuesta rápida y la proactividad (solución de problemas antes de que ocurran). Para ello es necesario tener operativas todas las herramientas de logging y reporting disponibles.

En cuanto a los métodos de validación, se diferenciarán dos partes: métodos de validación para la fase de testeo y métodos de validación para el entorno de producción. Para la fase de testeo se realizará una implementación de todo el sistema desde cero, incluyendo la preparación del entorno físico, por lo que se realizará una validación de cada paso realizado a medida que vaya avanzando el proyecto. La fase de producción, al contrario, se realizará de forma planificada, coordinada y juntamente con el departamento que colabora en el proyecto.

Para el seguimiento y coordinación del proyecto se utilizarán herramientas como Trello (planning y seguimiento de tareas) y una aplicación propietaria para la gestión del tiempo. Se utilizarán Microsoft Teams, para compartir de manera sencilla la documentación del proyecto, y Word para dar formato final. Además, se ha utilizado la aplicación draw.io[1] para crear los diagramas.

[1] https://www.draw.io/

Planificación temporal

5.1 Descripción de tareas

Dado que el objetivo principal del proyecto es la implementación de un sistema en un entorno en producción, es necesario definir las fases en las que se desarrollará. En una primera fase, y durante la familiarización con el entorno de trabajo, se preparará el entorno de pruebas, teniendo en cuenta los requisitos del sistema a implementar. Seguidamente, se realizará la fase de pruebas, momento en el que se comprobarán las funcionalidades que el sistema ofrece. Una vez completadas las pruebas en el entorno de pruebas, se dará inicio a la fase más crítica: la implementación en el entorno real, que incluirá pruebas antes de la implementación final.

5.1.1 Preparación del entorno de pruebas

La primera fase del proyecto cubre desde la preparación de los equipos físicos necesarios para la instalación del sistema, hasta la instalación de ésta. La idea inicial era crear el entorno utilizando virtualización anidada como se muestra en la Figura 5.1. Sin embargo, al realizar el estudio de requisitos del sistema se llegó a la conclusión de que los recursos hardware del host de virtualización que se iba a utilizar eran insuficientes para el sistema SCCVM y para posteriormente alojar máquinas virtuales para realizar las pruebas de la segunda fase. Por este motivo se inició la preparación y configuración de: dos hosts de virtualización, de la VM que actuará como controlador de dominio y del sistema de almacenamiento compartido. Así pues, la infraestructura del entorno final de testing es el que se muestra en la Figura 4.2. Esta fase se completó entre julio y principios de octubre.

Los recursos necesarios para esta fase serán:

i. Recursos humanos: técnico junior, encargado de preparar el entorno, y técnico senior para supervisar la preparación.
ii. Recursos Software: Licencias de Windows Server 2016, de *SCVMM* de pruebas y de Office para la documentación. Se usarán también varias herramientas para complementar la documentación tales como: draw.io, GanttProject, Trello, Google Drive, etc.
iii. Recursos Hardware: hosts de virtualización y NAS para el almacenamiento compartido. Se usará también un ordenador personal para todas las tareas.

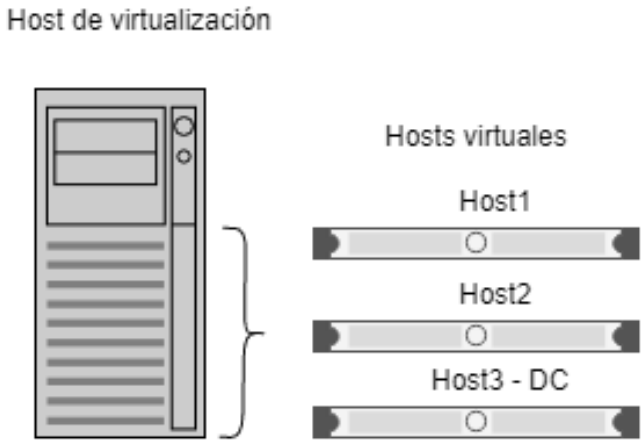


Figura 5.1: Entorno de pruebas; idea de infraestructura original.

5.1.2 Pruebas del sistema *SCVMM*

Una vez preparado el entorno de pruebas, se prevén aproximadamente dos meses de pruebas del sistema, entre octubre y noviembre, durante los cuales se harán pruebas exhaustivas de permisos de usuarios, de VMs, de redes virtuales, de copias de seguridad y de fallos del sistema.

Todos los recursos necesarios para esta fase serán los mismos que para la fase anterior.

5.1.3 Implementación del sistema *SCVMM*

Al terminar la fase de pruebas, dará comienzo la fase de implementación. Durante esta fase, las tareas irán desarrollándose con una planificación previa. Se empezará realizando un estudio de los pasos a seguir para la continuidad del negocio. Una vez hecho esto, se instalará el sistema. En este caso, no será necesario verificar los requisitos mínimos puesto que, una vez realizado el estudio para el entorno de pruebas, es seguro que el entorno real posee recursos más que suficientes para la instalación. Posteriormente se dará inicio a las tareas de preparación del entorno para la utilización del sistema (diseño y creación de la estructura necesaria) para poder realizar pruebas previas a la implementación final. Todo el proceso deberá documentarse. Se prevé que esta fase se realice entre finales de noviembre y mediados de enero.
Los recursos necesarios para esta fase serán:

i. Recursos humanos: técnico junior, encargado de la implementación del sistema con la supervisión de un técnico senior.
ii. Recursos Software: Licencias de Windows Server 2016, de *SCVMM* de pruebas y de Office para la documentación.
iii. Recursos Hardware: infraestructura *Cloud* donde realizar la implementación.

5.1.4 Diagrama de Gantt

La Figura 5.2 muestra la planificación temporal inicial de las tareas a realizar, y la Figura 5.3 su correspondiente diagrama de Gantt. El tiempo previsto para la realización de las tareas es de 20 horas semanales.

Nombre	Fecha de inicio	Fecha de fin
Aprendizaje inicial y familiarización con el entorno	2/07/18	30/07/18
Preparación entorno de pruebas	11/07/18	28/09/18
Estudio requisitos del sistema SCVMM	11/07/18	13/07/18
Preparación inicial entorno físico y virtual	16/07/18	17/08/18
Preparación final del entorno e instalación del sistema	3/09/18	28/09/18
Fase de pruebas	1/10/18	23/11/18
Pruebas de permisos de usuarios	1/10/18	12/10/18
Pruebas máquinas virtuales	15/10/18	26/10/18
Pruebas redes virtuales	29/10/18	9/11/18
Pruebas copias de seguridad y fallos sistema	12/11/18	23/11/18
Fase de implementación	26/11/18	4/01/19
Estudio para continuidad de negocio	26/11/18	30/11/18
Instalación del sistema SCVMM en entorno real	3/12/18	7/12/18
Preparación del entorno para prueba real	10/12/18	14/12/18
Pruebas en entorno real	17/12/18	28/12/18
Documentación final	24/12/18	4/01/19
Gestión del proyecto	17/09/18	15/10/18
Contexto y alcance	17/09/18	25/09/18
Planificación temporal	26/09/18	1/10/18
Gestión económica y sostenibilidad	2/10/18	5/10/18
Documento final	8/10/18	15/10/18
Documento específico especialidad	8/10/18	15/10/18

Figura 5.2: planificación temporal inicial.

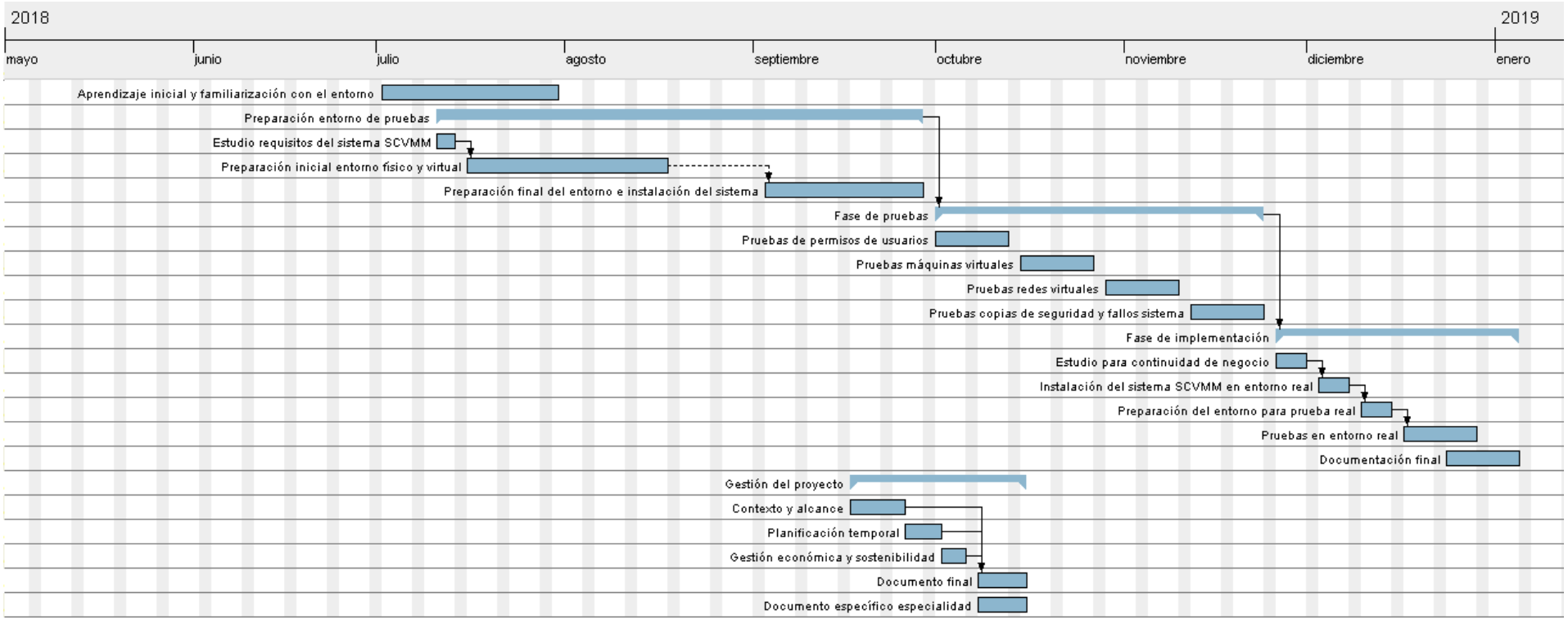


Figura 5.3: Diagrama de Gantt inicial.

Sin embargo, a medida que avanzaba el proyecto, se debió priorizar en algunas de las capacidades de *VMM* para poder finalizar a tiempo, por lo que algunas de las pruebas continuarán realizándose una vez el sistema se encuentre en producción. La planificación final es la que se muestra en la Figura 5.4, y su correspondiente diagrama de Gantt se muestra en la Figura 5.5.

Nombre	Fecha de inicio	Fecha de fin	Duración
Aprendizaje inicial y familiarización con el entorno	2/07/18	30/07/18	21
Preparación entorno de pruebas	11/07/18	28/09/18	58
Estudio requisitos del sistema SCVMM	11/07/18	13/07/18	3
Preparación inicial entorno físico y virtual	16/07/18	17/08/18	25
Preparación final del entorno e instalación del sistema	3/09/18	28/09/18	20
Fase de pruebas	1/10/18	1/02/19	90
Pruebas de permisos de usuarios	1/10/18	12/10/18	10
Pruebas máquinas virtuales	15/10/18	26/10/18	10
Pruebas redes virtuales	29/10/18	9/11/18	10
Realización de más pruebas	12/11/18	1/02/19	60
Fase de implementación	3/12/18	1/02/19	45
Estudio para continuidad de negocio	3/12/18	7/12/18	5
Instalación del sistema SCVMM en entorno real	10/12/18	14/12/18	5
Preparación del entorno para prueba real	17/12/18	21/12/18	5
Pruebas en entorno real	24/12/18	4/01/19	10
Documentación final	21/01/19	1/02/19	10
Gestión del proyecto	17/09/18	15/10/18	21
Contexto y alcance	17/09/18	25/09/18	7
Planificación temporal	26/09/18	1/10/18	4
Gestión económica y sostenibilidad	2/10/18	5/10/18	4
Documento final	8/10/18	15/10/18	6
Documento específico especialidad	8/10/18	15/10/18	6

Figura 5.4: planificación temporal final.

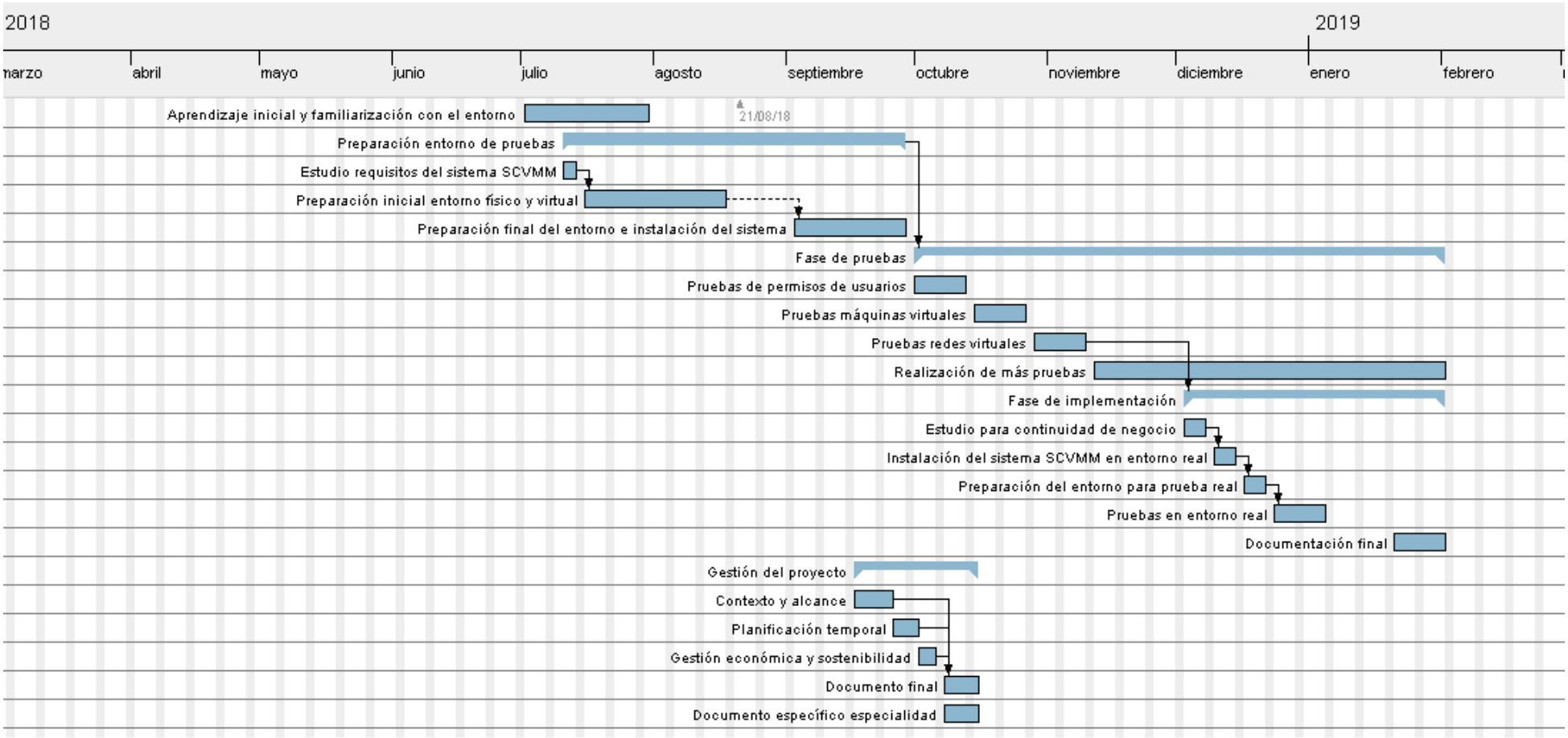


Figura 5.5: Diagrama de Gantt final.

5.2 Alternativas y plan de acción

Al tratarse de un proyecto de implementación del sistema *SCVMM* en un entorno actualmente en producción, es probable que la planificación no sufra apenas cambios o que sean muy leves. Estas desviaciones podrían ser:

i. **Requisitos del sistema:** Es posible que haya que hacer cambios en la infraestructura de testing debido a los requisitos del sistema durante la fase de pruebas. De igual manera que al realizar el estudio de requisitos se llegó a la conclusión de que hacía falta un host con más recursos hardware, durante la fase de pruebas puede ocurrir que ciertas funcionalidades requieran de más recursos para ejecutarse. Puede suceder también que se necesite alojar más VMs, y por tanto en algún momento los recursos no sean suficientes. Dado el caso, sería necesario preparar más hosts de virtualización para poder continuar con las pruebas.

ii. **Paradas del servicio para la implementación en entorno *Cloud*:** Durante la fase de implementación de *SCVMM* en el entorno real, fase más crítica del proyecto, y tal y como se ha comentado anteriormente, es posible que sea necesario realizar paradas del servicio actuando de una manera determinada. Para realizar una parada de servicio es necesaria una planificación sobre:

    a. Qué cambios hay que realizar.
    b. Cuándo hay que realizar los cambios (paradas programadas).
    c. Cuánto tiempo estará detenido el servicio.

    La manera en la que esto afectaría a la planificación temporal está relacionada con los puntos 2 y 3, ya que para poder realizarlos se debe notificar previamente a los clientes afectados. Una vez notificados, se les debe conceder unos días de margen para poder asegurar que les afecte en la menor medida posible. De esta forma, existe la posibilidad que se deba retrasar la detención del servicio por petición expresa de los clientes.

Gestión económica

6.1 Identificación y estimación de los costes

En esta sección se hace una estimación de los costes de los elementos que componen el presupuesto del proyecto diferenciando entre costes directos, costes indirectos e imprevistos.

6.1.1 Costes directos

La estimación de costes directos se hace distinguiendo los diferentes recursos: humanos, software y hardware.

6.1.1.1 Recursos humanos

El proyecto lo desarrollará una sola persona, con rol de técnico junior, con la supervisión de un técnico senior. Se estima el coste estimado de ambos teniendo en cuenta la remuneración y las horas de las tareas especificadas en el diagrama de Gantt visto en apartados anteriores, tal y como se muestra en la Tabla 6.1.

Rol	Horas estimadas	Remuneración (€/h)	Coste estimado (€)
Técnico junior	476 horas	15€/h	7140€
Técnico senior	142 horas	28€/h	3976€
TOTAL		**11116€**	

Tabla 6.1: Presupuesto de recursos humanos.

6.1.1.2 Recursos Software

El cálculo de la vida útil de los productos software utilizados en el proyecto, se ha hecho de dos maneras distintas: según si la licencia es de pago único o en cuotas. Por ejemplo, el Office 365 Empresa Premium tiene una vida útil de un año puesto que la licencia utilizada es anual y el proyecto terminará antes que sea necesario renovarla. Para otros productos, como por ejemplo para Windows Server 2016 Datacenter, se ha utilizado el tiempo hasta que el proveedor (en nuestro caso siempre será Microsoft) deja de ofrecer soporte[1]. El presupuesto estimado se muestra en la Tabla 6.2.

[1] Conocido como End of Life (EOL): https://support.microsoft.com/en-us/lifecycle/search/19616

Software	Precio	Unidades	Vida útil	Amortización estimada (6 meses)
Drive	0€	-	-	-
Trello	0€	-	-	-
GanttProject	0€	-	-	-
draw.io	0	-	-	-
Hyper-V	0€	-	-	
Office 365 Empresa Premium	108.66€	1	1 año	54.33€
Windows Server 2016 Datacenter 16 cores (hosts)	3849.95€	2	8 años	240.62 €
Windows Server 2016 Standard (DC)	540.98€	1	8	33.81€
SCVMM versión de prueba	0€	1	180 días	0€
SCVMM	3133,92€	1	8 años	195.87€
TOTAL		**524.63€**		

Tabla 6.2: Presupuesto de recursos Software.

6.1.1.3 Recursos Hardware

En este proyecto la mayoría de los recursos hardware son reutilizados y totalmente amortizados, por lo que el coste real de éstos es 0€. En la Tabla 6.3 se muestra, sin embargo, una estimación de lo que costaría en caso de necesitar comprar todos los componentes. Para todos los componentes se ha estimado una vida útil de 4 años.

Producto	Precio por unidad	Unidades	Precio estimado	Vida útil	Coste real	Amortización estimada (6 meses)
Servidor ML350 Gen10 32GB RAM con 2 discos 300GB	2475.41€	2	4950.82€	4	0€	0€
Switch 24P GS1920	135.62€	1	135.62€	4	0€	0€
NAS TS-863XU	1197.64€	1	1197.64€	4	0€	0€
Disco SSD 480GB	76.65€	2	153.3€	4	0€	0€
Disco Toshiba HDD 4TB	101.53€	2	203.06€	4	0€	0€
Ordenador personal	200€	1	200€	4	0€	0€
TOTAL			**0€**			

Tabla 6.3: Presupuesto de recursos Hardware.

6.1.2 Costes indirectos

La realización del proyecto requiere el uso de energía e internet durante todas las fases. Además, para la fase de implementación se debe tener en cuenta el coste de mantener la infraestructura en el centro de datos. Sin embargo, el proyecto no incrementaría el coste de este servicio, ya que se está utilizando para otras tareas.

Servicio	Precio	Tiempo	Coste estimado
Consumo eléctrico oficina	350€/mes	6 meses	2100€
Acceso a Internet	40€/mes	6 meses	240€
Servicio infraestructura CPD	700€/mes	2 meses	1400€
TOTAL	**3740€**		

Tabla 6.4: Presupuesto de costes indirectos.

6.1.3 Imprevistos

Existiría la posibilidad de requerir una licencia de SQL Server 16 cores según la cantidad de información que el sistema *SCVMM* requiera almacenar. En el entorno real ya se está

utilizando, por tanto, se utilizará la ya existente mientras sea posible. En caso de requerir otra, el coste de esta sería el que se muestra en la Tabla 6.5.

Software	Precio	Unidades	Vida útil	Amortización estimada (6 meses)
SQL Server 16 cores	566.10€	1	8 años	35.38€
TOTAL				**35.38€**

Tabla 6.5: Presupuesto de costes imprevistos.

6.1.4 Coste total del proyecto

Con las estimaciones anteriores, y teniendo en cuenta una contingencia del 8%, el coste total del proyecto quedaría como se muestra en la Tabla 6.6.

Concepto	Coste
Costes directos	11640.63€
Costes indirectos	3740€
Contingencia (8%)	1230.45€
Costes imprevistos	35.38€
TOTAL	**16646,46€**

Tabla 6.6: Presupuesto total.

6.2 Control de gestión

Las posibles desviaciones en el presupuesto del proyecto serán principalmente de recursos humanos, puesto que el tiempo de realización del proyecto es lo que varía con mayor frecuencia. Por otro lado, en cuanto a los recursos software, la posible desviación que puede producirse es la necesidad de requerir una licencia distinta del sistema *SCVMM*[1]. Por último, en referencia a los recursos hardware, es necesario mantener una revisión constante para prevenir cualquier tipo de avería y así evitar gastos innecesarios.

[1] Su precio varía según los recursos hardware del procesador del equipo donde se utilice.

Sostenibilidad y compromiso social

7.1 Dominio actual de la competencia de sostenibilidad

El objetivo del cuestionario es reflejar la necesidad tener en cuenta las tres dimensiones (social, medioambiental y económica) en la realización de proyectos TIC. En unas primeras preguntas se pretende conocer el nivel de conocimiento en el ámbito de la sostenibilidad. En general, estoy de acuerdo con todas ellas, aunque no con el nivel que me gustaría.

En cuanto a la dimensión ambiental, comprendo el impacto, tanto positivo como negativo, que los proyectos TIC tienen en la sociedad y en la sostenibilidad y me esfuerzo por tenerlo en cuenta en la realización de los proyectos. Sin embargo, desconozco las técnicas para medir este impacto.

Con respecto a la dimensión social, conozco las problemáticas asociadas a la accesibilidad, ergonomía, justicia social, equidad, etc. y comprendo la necesidad de introducirlos en los proyectos TIC. A pesar de esto, no conozco los indicadores para medir la contribución del proyecto en la sociedad.

En relación con la dimensión económica, conozco los procesos de gestión de proyectos y las diferentes partes económicas que tienen, pero flaqueo en la gestión económica durante toda su vida útil. Las últimas preguntas tienen que ver con herramientas colaborativas y ética profesional. Tengo conocimiento sobre herramientas colaborativas, que utilizo, y sobre el impacto que tienen en el desarrollo de un proyecto TIC. En cuanto a los principios éticos, conozco los conceptos, pero generalmente no los tengo en cuenta en el momento de desarrollar proyectos.

Para concluir, entre mis puntos fuertes destacaría el conocimiento sobre la sostenibilidad en sus tres dimensiones e intentar tenerlos en cuenta en la realización de proyectos TIC. Entre mis debilidades y por tanto lo que debería desarrollar, está el desconocimiento de indicadores para medir el impacto medioambiental, social y económico.

7.2 Dimensión económica, social y ambiental

Para la dimensión económica, el coste estimado para la realización del proyecto tiene en cuenta tanto recursos humanos como materiales, tal y como se muestra en apartados anteriores. Con más experiencia y conocimiento en el ámbito, se podría realizar en mucho menos tiempo y por tanto menos recursos humanos. Sin embargo, no se reduciría el coste de los recursos software, ya que son en su mayoría gratuitos, o con un coste no dependiente del tiempo, ni de los recursos hardware que son prácticamente todos reutilizados.

En relación con la dimensión social, hay una necesidad real del proyecto, ya que se trata de una implementación que la propia empresa necesita. Una de las finalidades del proyecto es sin duda facilitar el trabajo de los usuarios, permitiendo la realización de las tareas de manera mucho más eficaz y sencilla. Además, el proyecto no perjudica a ningún colectivo.

Por último, en cuanto a la dimensión ambiental, los recursos necesarios durante las diferentes fases del proyecto son los que se detallan en la estimación del presupuesto. El consumo principal durante la realización del proyecto y posteriormente será el consumo eléctrico. Durante las dos primeras fases principalmente consumirán los dos hosts de virtualización. Sin embargo, este consumo es una pequeña parte del consumo total de la oficina donde se realizarán. En la fase de implementación, el sistema se alojará en un centro de procesamiento de datos (en adelante CPD), donde el consumo será una parte muy pequeña del consumo total del centro. Como se ha mencionado anteriormente, durante las dos primeras fases se están reaprovechando prácticamente todos los recursos hardware. Una vez terminado el proyecto, todo el hardware utilizado durante la fase de pruebas se podrá aprovechar, puesto que el sistema quedará implementado en el entorno de producción.

Desarrollo del proyecto: Preparación del entorno

En los siguientes apartados se explicará el desarrollo del proyecto fase por fase. Para empezar, se realizará el estudio de requisitos para instalar el sistema *SCVMM*. A continuación, se realizará la preparación de los hosts de virtualización, donde se crearán las VMs en las que se instalará el sistema *SCVMM*. Seguidamente se realizarán las pruebas de la herramienta. Estas pruebas a grandes rasgos consistirán en:

i. Prueba de plantillas para desplegar VMs.
ii. Gestión de las redes virtuales.
iii. Administración del entorno mediante permisos de usuarios y grupos.
iv. Pruebas de respuesta con fallos del sistema.

Por último, una vez concluidas las pruebas, se realizará la planificación e implementación en el entorno real del sistema *SCVMM.*

8.1 Estudio de requisitos

Antes de preparar los equipos físicos necesarios, se debe realizar un estudio de requisitos para conocer los recursos necesarios. Este estudio nos lo ofrece Microsoft y se muestra en las Tablas 8.1 a 8.6.

Hardware				
Hardware	Servidor *VMM*	Base de datos de *VMM*	Biblioteca de *VMM*	Consola de *VMM*
Procesador (mínimo)	Pentium 4 de 8 núcleos a 2 GHz (x64)	Pentium 4 de 8 núcleos a 2,8 GHz	Pentium 4 de 4 núcleos a 2,8 GHz	CPU de 2 núcleos, Pentium 4, 1 GHz
Procesador (recomendado)	CPU de 16 núcleos, 2,66 GHz	CPU de 16 núcleos, 2,6 GHz	CPU de 4 núcleos, 2,8 GHz	CPU de 2 núcleos, 2 GHz
RAM (mínimo)	4 GB	8 GB	2 GB	4 GB
RAM (recomendado)	16 GB	16 GB	4 GB	4 GB
Unidad de disco duro (mínimo)	4 GB	50 GB	Basado en tamaño/cantidad de archivos almacenados	10 GB
Unidad de disco duro	10 GB	200 GB		10 GB

Tabla 8.1: Requisitos hardware.

Como se ha mencionado en apartados anteriores, la idea original del proyecto era utilizar un único host en el que crear las VMs para ejecutar el sistema. Finalmente hemos podido disponer de dos hosts de virtualización, uno con 16GB de RAM y el segundo con 24GB de RAM. Los procesadores superan en rendimiento a lo mínimo establecido:

i. Primer host: Intel Xeon E5-606 de 4 núcleos

ii. Segundo host: Intel Xeon E5-2620 de 8 núcleos.

Por último, el sistema de almacenamiento compartido consiste en un NAS con conexión *iSCSI* (SAN), en el que disponemos de 2TB para almacenar las VMs y de esta forma hacerlas de alta disponibilidad (si cayese un host, el otro podría acceder a sus archivos de configuración y disco duro virtual).

Sistema operativo de servidor			
Sistema operativo	Servidor *VMM*	Biblioteca *VMM* remota	Base de datos *VMM* remota
Windows Server 2012 R2 Standard/Datacenter	No	Si	Si es compatible con la versión de SQL Server
Windows Server 2016	Si	No	
Windows Server 2016 (con experiencia de escritorio)	Si	Si	
Windows Server 1709	Si	Si	Si

Tabla 8.2: Sistemas operativos compatibles del servidor de *VMM*.

Sistema operativo de la consola de *VMM*	
Sistema operativo	Compatible
Windows 10 Enterprise	Si
Windows Server 2012 R2 Standard, Datacenter	Si
Windows Server 2016 Standard, Datacenter	Si

Tabla 8.3: Sistemas operativos compatibles de la consola de *VMM*.

Tanto los hosts como las VMs para el sistema tienen instalado el sistema operativo Windows Server 2016 Standard con experiencia de escritorio que, como se ve en la Tabla 8.2, es compatible para todos los componentes de *VMM*.

SQL Server	
Versión de SQL	Compatible
SQL Server 2008	No
SQL Server 2012	Si
SQL Server 2014	Si
SQL Server 2016	Si
SQL Server 2017	Si
Utilidades de línea de comandos de SQL Server	Realice la instalación en el servidor *VMM* si desea implementar las aplicaciones de capa de datos de SQL Server en el tejido de *VMM*. No necesario para la instalación de *VMM*.

Tabla 8.4: compatibilidad de la base de datos.

La versión de SQL Server utilizada es la de 2016 que, como se observa en la Tabla 8.4, es compatible con *SCVMM* 2016.

Virtualización	
Máquina Virtual	Compatible
Servidor de administración *VMM*	El servidor de administración *VMM* se puede instalar en una máquina virtual. Si utiliza la memoria dinámica, establezca la RAM de inicio de la máquina virtual en al menos 2048 MB. No realice la instalación en un servidor con Hyper-V. Puede implementar el servidor de administración de *VMM* (físico o máquina virtual) en un clúster de alta disponibilidad.
Consola *VMM*	Puede instalar la consola *VMM* en una máquina virtual.

Tabla 8.5: Compatibilidad de la instalación del sistema en VMs.

En la Tabla 8.5 se confirma uno de los puntos más importantes de este estudio: el sistema se puede instalar en VMs para así evitar tener que utilizar un host por cada componente de *VMM*.

Componentes de instalación		
Componente	Servidor *VMM*	Consola de *VMM*
Active Directory	El servidor de administración *VMM* debe ser un miembro del dominio. El nombre del equipo no debe superar los 15 caracteres	Un equipo con la consola *VMM* instalada debe ser un miembro del dominio.
Windows ADK	Requiere Windows ADK para Windows 10	No aplicable
PowerShell	PowerShell 5.0	PowerShell 4.0 5.0
.Net	4.6	4.5, 4.5.1, 4.5.2, 4.6

Tabla 8.6: Componentes necesarios para la instalación de *SCVMM*.

En la Tabla 8.6, se detallan algunos componentes que deben instalarse en la VM que ejercerá de servidor *VMM*, previamente al sistema *SCVMM*. Uno de estos componentes nos indica que el servidor *VMM* y la consola deben ser miembros del dominio. Por este motivo es necesario ubicar una VM fuera de los hosts con el rol de Active Directory para poder crear un dominio de test y unir tanto a los hosts como a las VMs a este. Debe estar fuera de los hosts ya que estos mismos van a pertenecer al dominio, y por lo tanto debe ser totalmente independiente a estos.

Por último, Microsoft también nos ofrece una lista de sistemas operativos y máquinas virtuales que se pueden gestionar desde este sistema. Los sistemas operativos compatibles son todos a partir de Windows Server 2012 R2, excluyendo Windows Server 2016 sin experiencia de escritorio. Aunque no será necesario en nuestro caso, también admite servidores de VMWare. En cuanto a las VMs que se pueden gestionar, cualquier máquina ejecutada en hosts de Hyper-V o VMWare son compatibles.

8.2 Preparación del entorno físico

Los componentes físicos se pueden preparar en paralelo casi en su totalidad. Sin embargo, las siguientes secciones se ordenan por dependencias, de manera que se detallarán primero los componentes cuyas configuraciones sean dependencia de otro. Dicho esto, lo primero que hay que preparar es la VM que ejerce de controlador de dominio y servidor DNS, seguido por el NAS para el almacenamiento compartido, y por último los hosts físicos, que deben poder unirse al dominio y conectarse al NAS mediante *iSCSI*.

8.2.1 Controlador de dominio y servidor DNS

Una breve explicación de lo que son un controlador de dominio y un servidor DNS es la siguiente:

i. Un controlador de dominio, en concreto Active Directory de Microsoft, se encarga de almacenar información de los objetos en la red (equipos, recursos…) y proporciona acceso a los usuarios a estos recursos.
ii. Un servidor DNS proporciona resolución de nombres para redes TCP/IP y se administra de manera más sencilla instalado en el mismo servidor que Active Directory, ya que trabajan de manera conjunta.

Para preparar el controlador de dominio (en adelante DC), se ha creado una VM mediante Hyper-V en un servidor local independiente. Para hacerlo simplemente hay que acceder al administrador de Hyper-V y crear una VM nueva. Este proceso se repetirá cuando se creen las VMs necesarias para el sistema *SCVMM*, y por tanto se detallará en este apartado. La Figura 8.1, muestra la interfaz de Hyper-V.

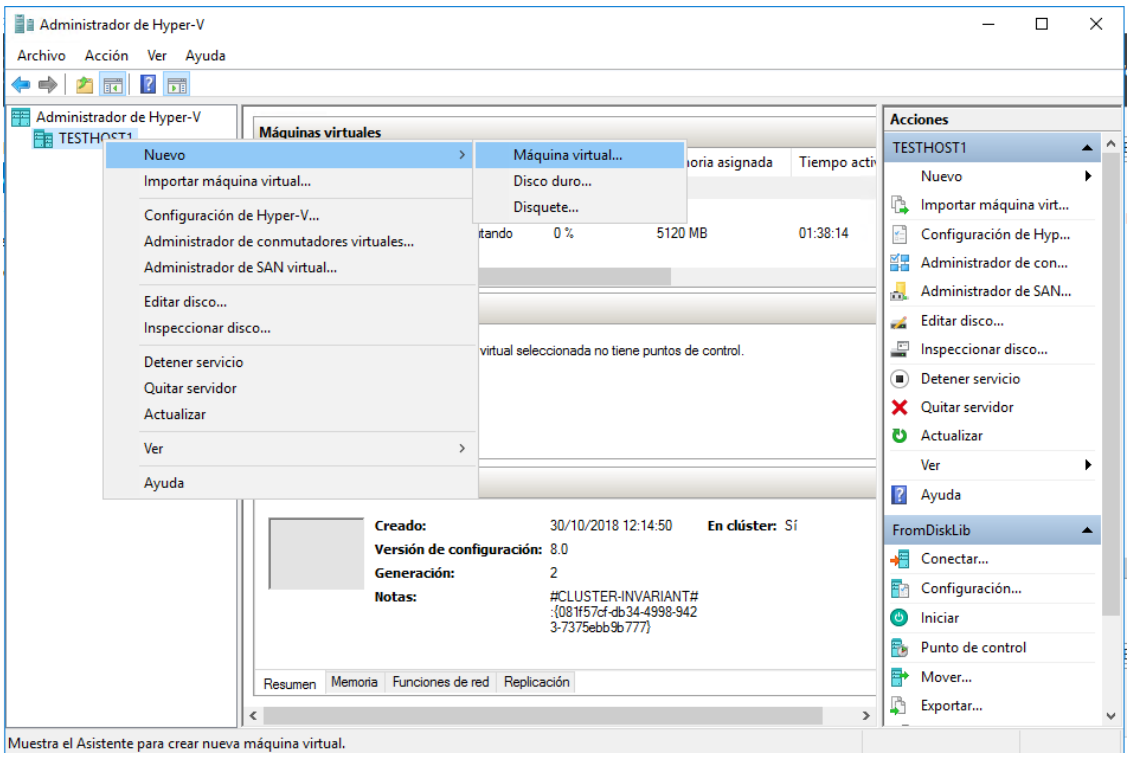


Figura 8.1: interfaz de Hyper-V para crear una VM nueva.

Después de esto, se abre un asistente donde se debe indicar:

i. Nombre de la VM: testdc
ii. Ubicación de la configuración de la VM: al ser la ubicación del DC/DNS, se ha ubicado en el disco local del servidor, C:/Hyper-V.
iii. Generación: 2.
iv. Memoria RAM: 3GB.
v. Conexión de red.
vi. Ubicación y tamaño del disco duro virtual (VHD) de la VM: C:/Hyper-V/VHD, 80GB.

Una vez listo, se debe crear la VM, pero sin S.O. Para instalarlo, se debe añadir la ISO de instalación. Para hacerlo simplemente hay que abrir la configuración de la VM recientemente creada, y añadir una unidad de DVD a la controladora SCSI como se muestra en la Figura 8.2.

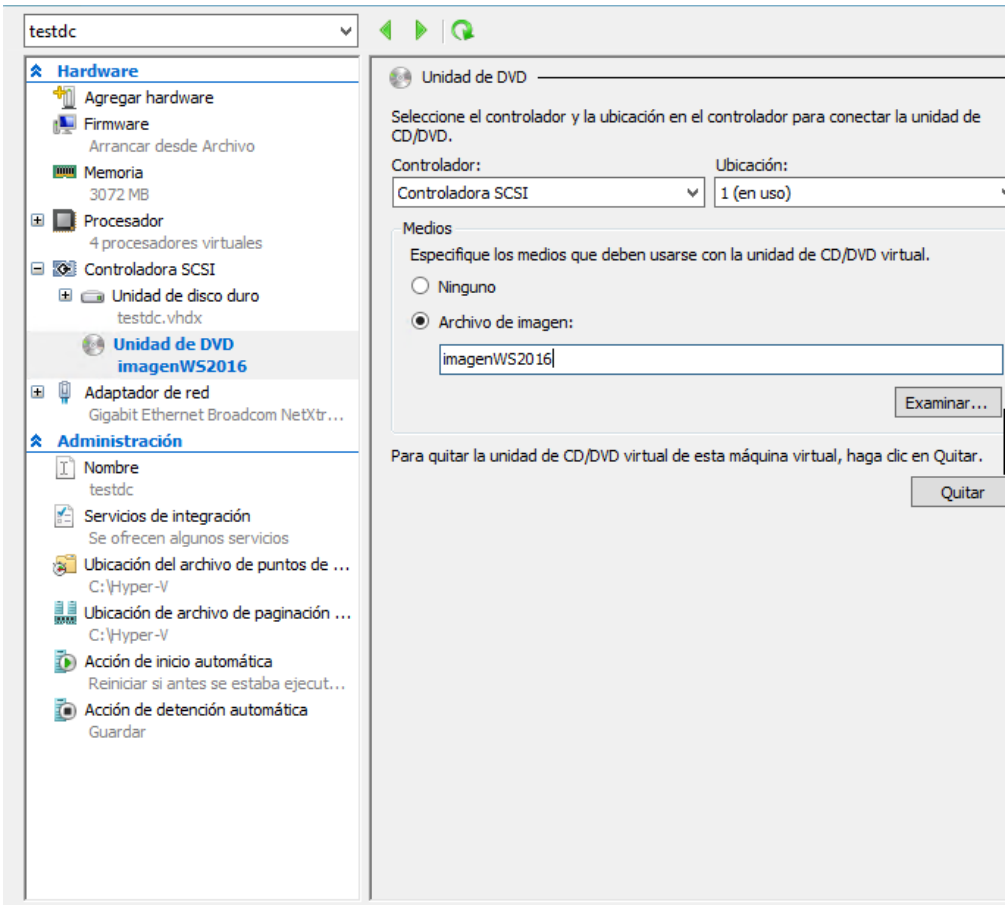


Figura 8.2: configuración de la VM para instalar el S.O.

Con la ISO preparada, se puede iniciar la máquina para proceder con la instalación. Una vez instalado el sistema operativo, el primer paso es comprobar si tiene actualizaciones pendientes, en cuyo caso se instalarán antes de continuar. Por último, es importante que esta VM disponga de una IP fija, para que los hosts puedan acceder a sus servicios, por tanto, se modifican las opciones de adaptador de red, modificando su IPv4 como muestra la Figura 8.3.

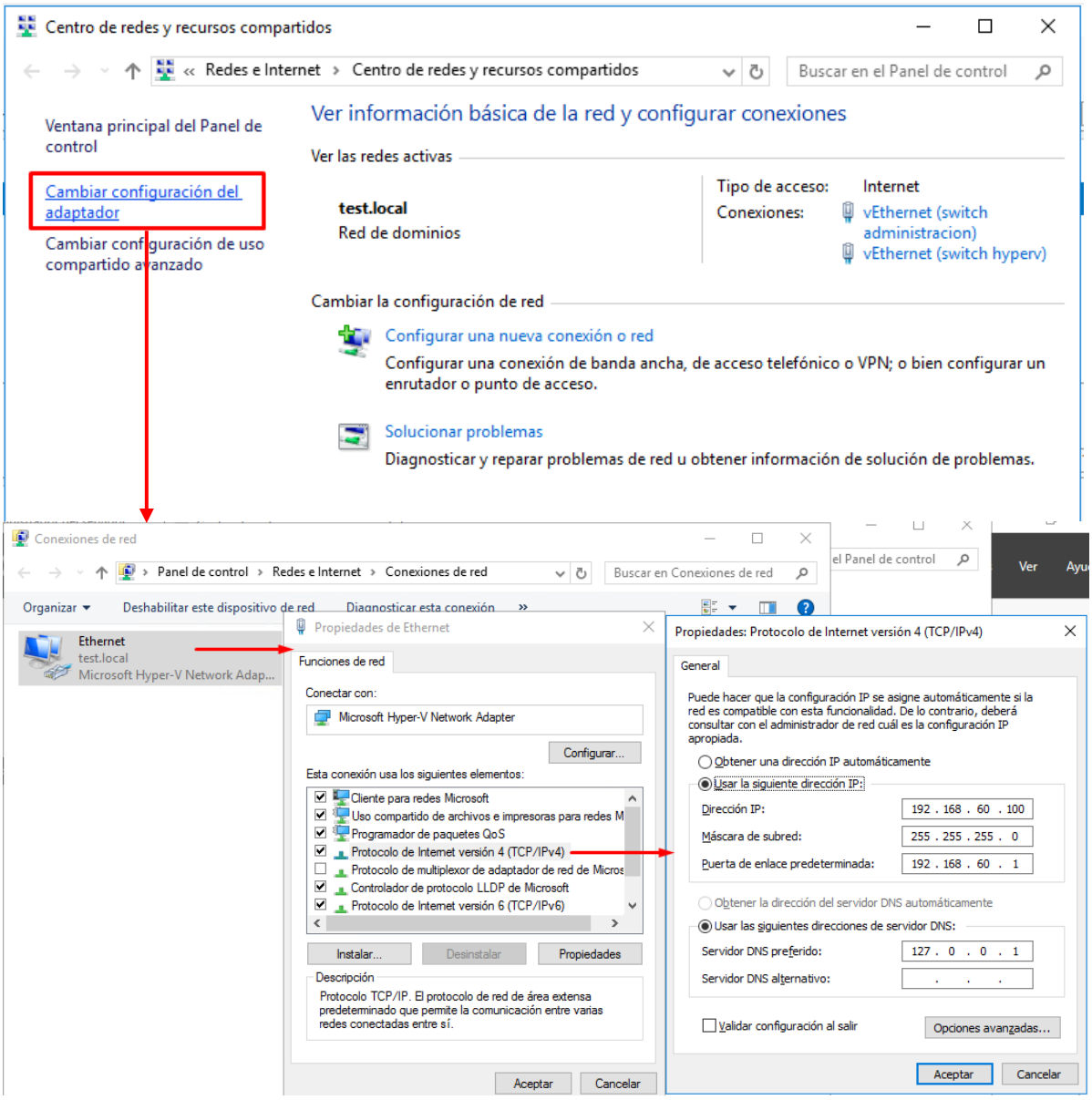


Figura 8.3: opciones de IPv4.

Las IPs utilizadas en el proyecto pertenecen al rango 192.168.60.X. La IP del servidor DNS para esta VM es la IP de loopback (su servidor DNS es la propia VM) y siendo su dirección IP la 192.168.60.100. Esta IP es la que los hosts y las VMs del sistema utilizan como servidor DNS. Una vez fijada la IP, se puede comenzar con la preparación de los roles de DC/DNS.

Para instalar los roles, se debe acceder al panel de administrador del servidor, y agregar un nuevo rol. Se ejecuta entonces un asistente, donde se debe seleccionar *Active Directory* y *DNS* en el apartado roles de servidor, y en la sección de características, .NET Framework y powershell. Es recomendable aplicar estas características en cualquier servidor nuevo, y por tanto se aplicarán también cuando se preparen los hosts físicos y las VMs del sistema *SCVMM*. Al haber seleccionado *Active Directory y DNS*, aparecen opciones de configuración, donde se debe especificar:

i. Añadir un nuevo bosque: test.local.
ii. Niveles funcionales de bosque y dominio: Windows Server 2016.
iii. Contraseña para modo de recuperación de servicios de directorio.
iv. Nombre de NetBIOS: TEST.

Nota

Siempre que no afecte a ningún otro servicio en ejecución en el mismo servidor, cuando se añada un rol es recomendable seleccionar la opción de reiniciar automáticamente, como muestra la Figura 8.4, por si hiciese falta para que la instalación sea completamente efectiva.

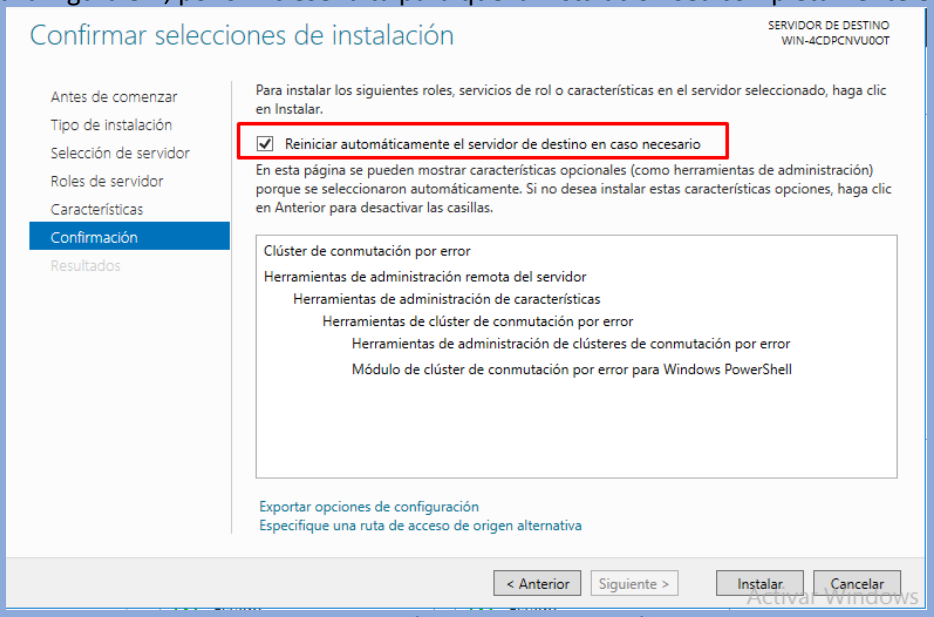


Figura 8.4: Opción de reinicio automático.

Nota

En entornos de producción es necesario disponer de un segundo DC/DNS como medida de seguridad frente a desastres.

El resto de la configuración del DNS se puede dejar con las opciones por defecto hasta la opción de reiniciar. Es recomendable añadir una zona DNS de búsqueda inversa (traduce IPs a nombres de equipos) al servidor DNS. Para añadirlo, se debe acceder al administrador de DNS, y crear una nueva zona en el apartado de zonas de búsqueda inversa, como muestra la Figura 8.5. Al hacerlo, se abre un asistente donde se especifica:

i. Zona principal.
ii. Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: test.local.
iii. Zona de búsqueda inversa para IPv4.
iv. Id. de red: 192.168.60.
v. Permitir solo actualizaciónes dinámicas seguras.

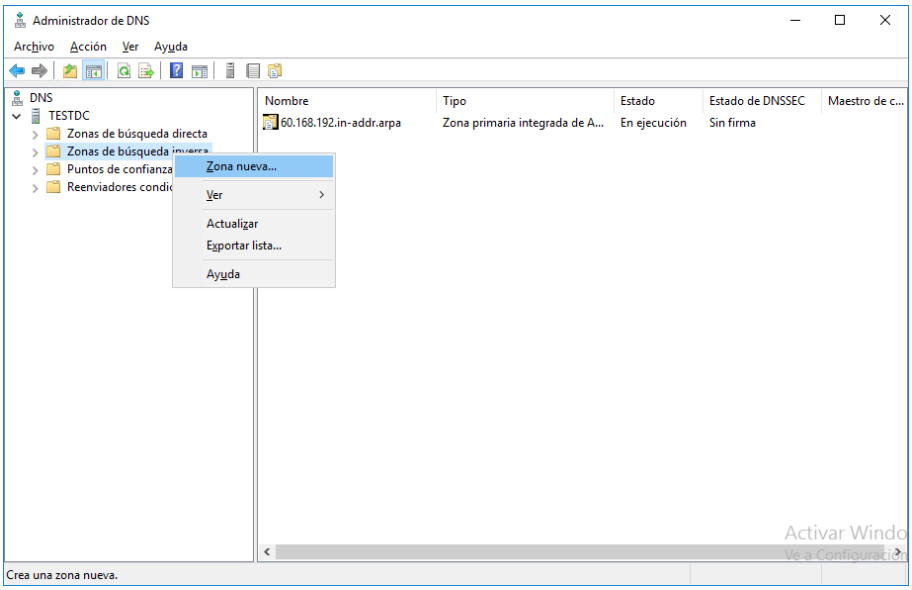


Figura 8.5: Creación de zona de búsqueda inversa.

Seguidamente, hay que modificar las directivas del dominio, para evitar que las contraseñas caduquen, que no deban cumplir cierta complejidad y para evitar que al modificar una contraseña no se puedan utilizar las contraseñas utilizadas anteriormente. Estos cambios se hacen para el entorno de testing, para evitar complicaciones al utilizar contraseñas. Sin embargo, por la nueva ley de protección de datos, es obligatorio mantener la configuración de complejidad en entornos de producción. Para realizar los cambios, se debe acceder al administrador de directivas de grupo, y editar las políticas por defecto como se muestra en la figura 8.6. Se abre una nueva ventana donde se pueden modificar estas propiedades, tal y como se muestra en la Figura 8.7.

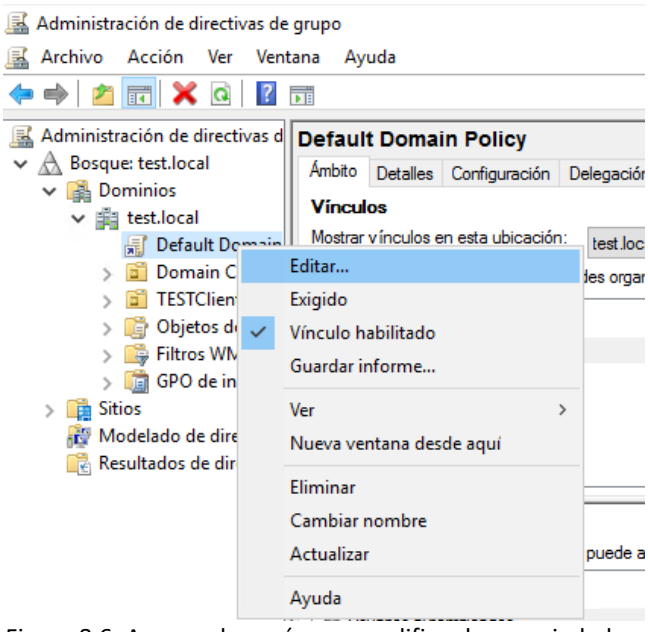


Figura 8.6: Acceso al menú para modificar las propiedades.

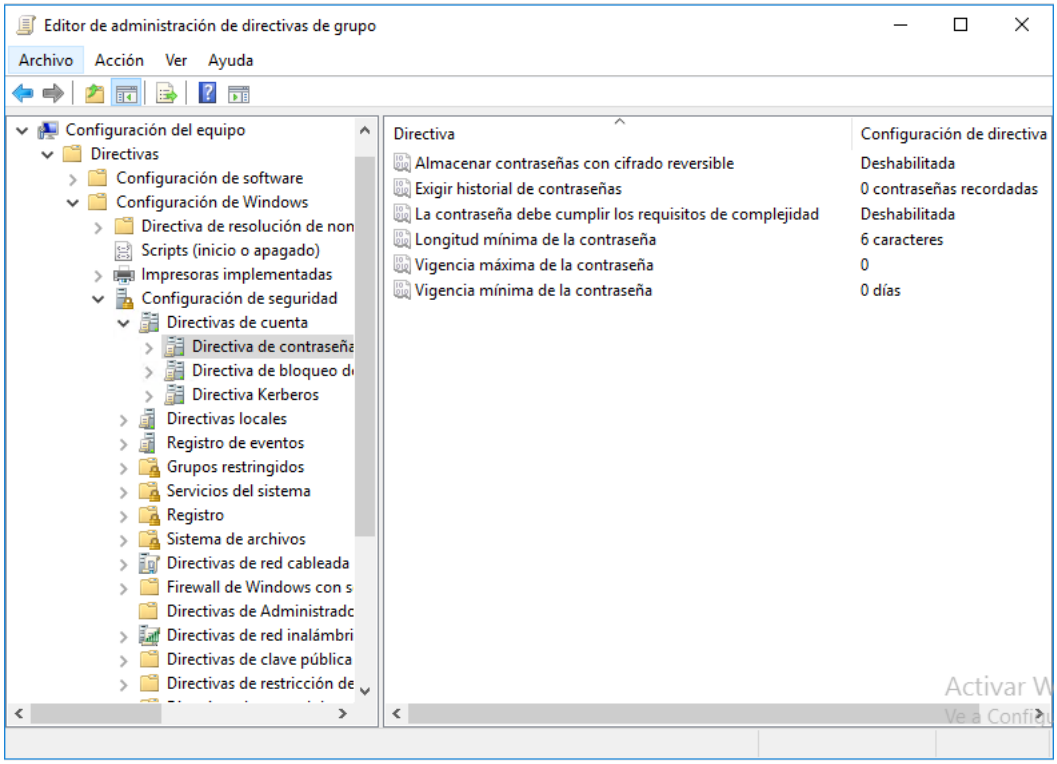


Figura 8.7: Menú de modificación de propiedades.

Por último, se crea el usuario administrador con el cual se accede a los servidores una vez agregados al dominio. Para ello, se debe abrir la herramienta *Usuarios y equipos de Active Directory* y crear un nuevo usuario, como muestra la Figura 8.8.

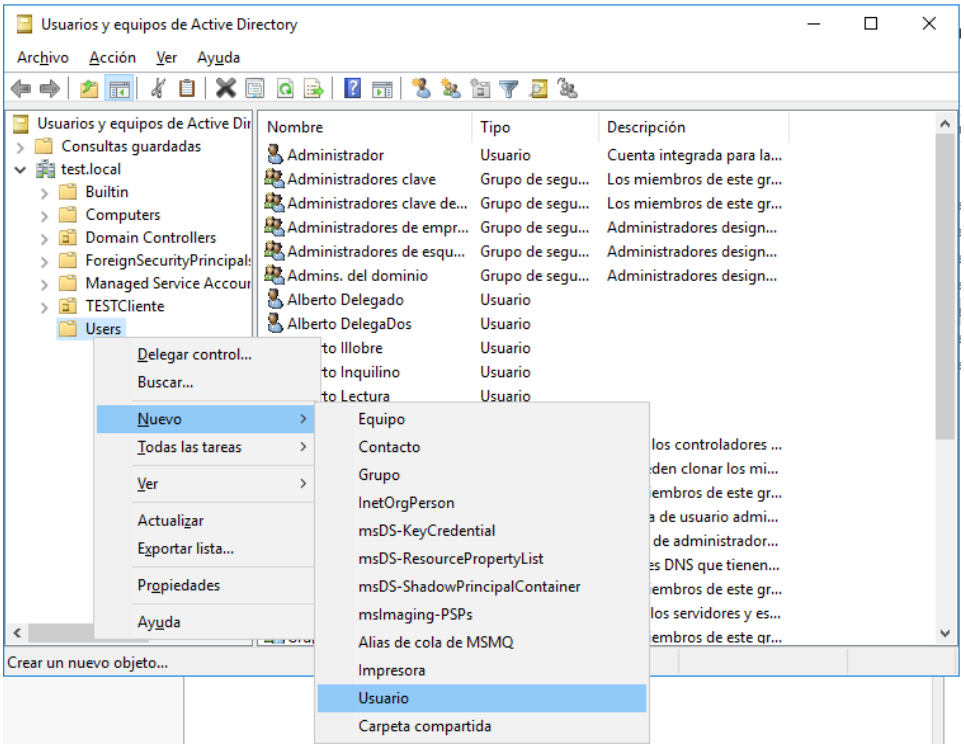


Figura 8.8: creación de un nuevo usuario.

En la ventana que se abre se debe especificar:

i. Nombre y Apellidos.
ii. Nombre de inicio de sesión de usuario (posterior y anterior a Windows 2000, recomendable usar el mismo).
iii. Contraseña: al establecer una contraseña se han establecido las siguientes opciones:
    a. Primera opción sin seleccionar: El usuario NO debe cambiar la contraseña en el siguiente inicio de sesión.
    b. Segunda opción sin seleccionar: El usuario PUEDE cambiar la contraseña.
    c. Tercera opción seleccionada: La contraseña nunca expira.
    d. Cuarta opción sin seleccionar: La cuenta está habilitada.

Este usuario es el utilizado para instalar y administrar la herramienta *VMM*, por tanto, se le ha nombrado VMMAdmin. Por último, tal y como indican los requisitos, para instalar *SCVMM*, el usuario debe tener permisos de administrador del dominio. Para que tenga estos permisos, se deben abrir las propiedades del nuevo usuario haciendo click derecho sobre este. Se abre una nueva ventana, en la cual hay que acceder a la pestaña de *Miembro de* y agregarle nuevos grupos. Al pulsar *Agregar* se abre una nueva ventana, en la cual lo más sencillo para añadir los grupos a los que pertenece es abrir las opciones avanzadas y pulsar en *Buscar ahora*. Aparecen entonces todos los grupos disponibles, entre los cuales los que se deben añadir son los que se muestran en la Figura 8.9.

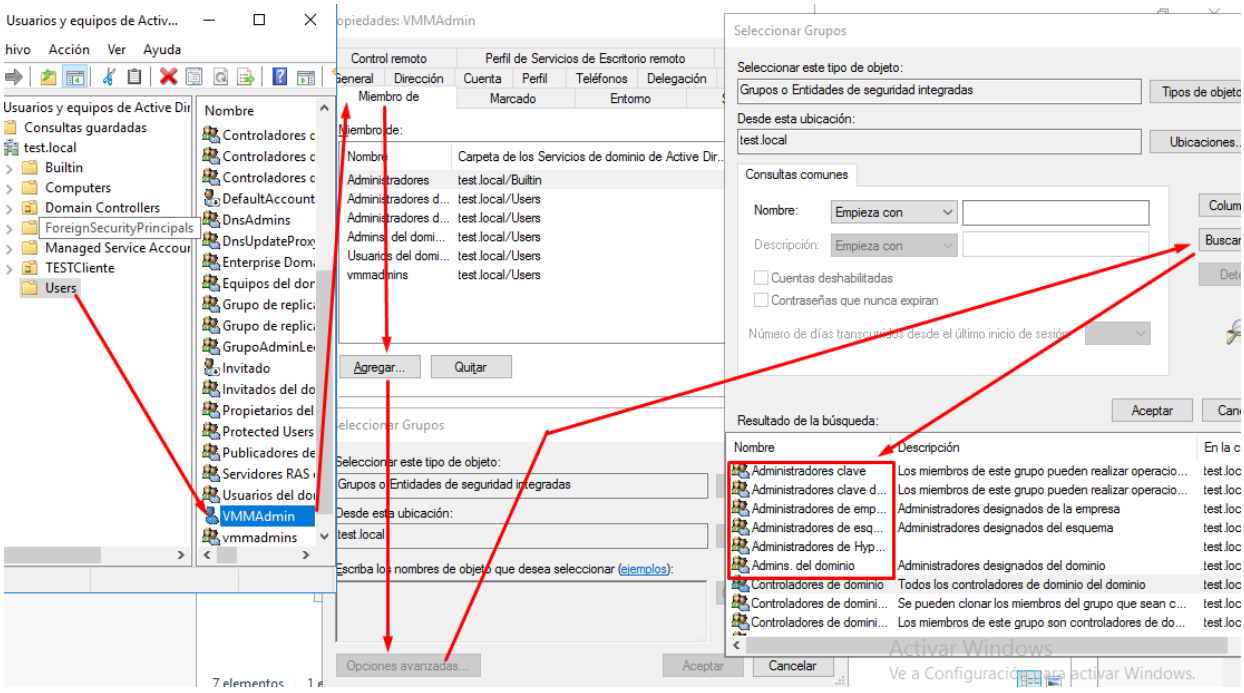


Figura 8.9: Grupos de administradores de dominio.

Con esto termina la configuración del DC, que se ha utilizado para crear nuevos usuarios para realizar las pruebas de la herramienta.

8.2.2 NAS para almacenamiento compartido

El siguiente componente que hay que preparar es el NAS. Para ello simplemente hay que acceder a su página de configuración. En nuestro caso es un NAS de QNAP, por lo que contamos con una aplicación que nos ayuda a encontrar el dispositivo en la red y acceder de manera sencilla. En la aplicación se puede observar algo similar a lo que muestra la Figura 8.10.

Figura 8.10: QNAP Finder para acceder al NAS.

Para configurar el NAS se puede hacer mediante la opción *Configuración* que aparece en la aplicación, o hacer doble click en el NAS. Una vez hecho, se puede configurar el NAS mediante web:

i. Nombre del NAS, contraseña de administrador.
ii. Escoger la zona horaria y sincronizarla con un servidor de tiempo: pool.ntp.org.
iii. Configuración de la IPv4 fija: 192.168.60.11
iv. Configuración de la puerta de enlace: 192.168.60.1.
v. Configuración del DNS: utilizaremos la IP fijada en el DC, es decir, 192.168.60.100.
vi. Configuración de disco: RAID 5.

Una vez hecho esto se aplicará la configuración y se puede acceder a la aplicación del NAS para configurar el almacenamiento por *iSCSI*. Para ello se accede a *Almacenamiento e instantáneas* tal y como se muestra en la Figura 8.11.

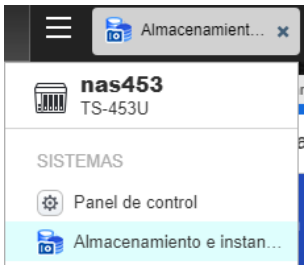


Figura 8.11: Acceso a la configuración del almacenamiento.

Un ejemplo de interfaz de un NAS Qnap se muestra en la Figura 8.12. Para realizar la configuración, se debe acceder a *Almacenamiento iSCSI*.

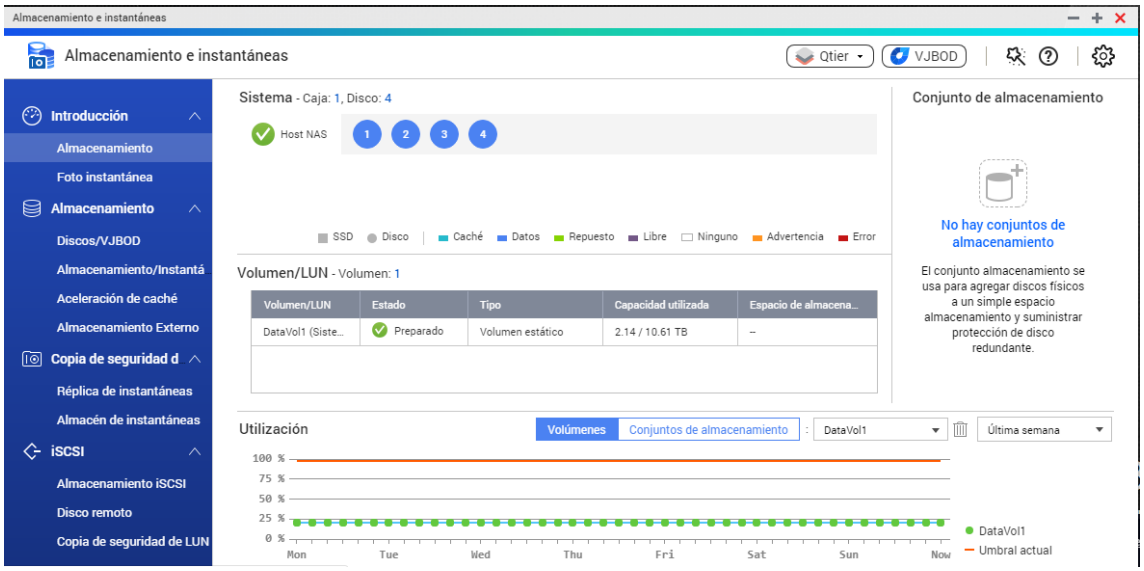


Figura 8.12: Interfaz del NAS para configuración de almacenamiento.

Una vez se haya accedido, se deben crear los objetivos *iSCSI* y sus LUNs (Logical Unit Number). Se le llama objetivo ya que los hosts conectarán al NAS mediante la herramienta *iniciador iSCSI*, y serán los encargados de iniciar la conexión con el dispositivo, el cual es su target u objetivo. Un LUN es una dirección para una unidad de disco duro y sirve para diferenciar unidades de disco individuales (una partición virtual) en un RAID de discos. Para ello se debe seleccionar la opción crear, y escoger *Objetivo iSCSI con un Lun asociado.* En los siguientes pasos, se puede nombrar al objetivo y LUN, además de limitar la capacidad que tendrá el LUN. El proceso completo en nuestro caso se detalla en las Figuras 8.13-8.17. Este proceso puede variar según la versión del NAS y el modelo.

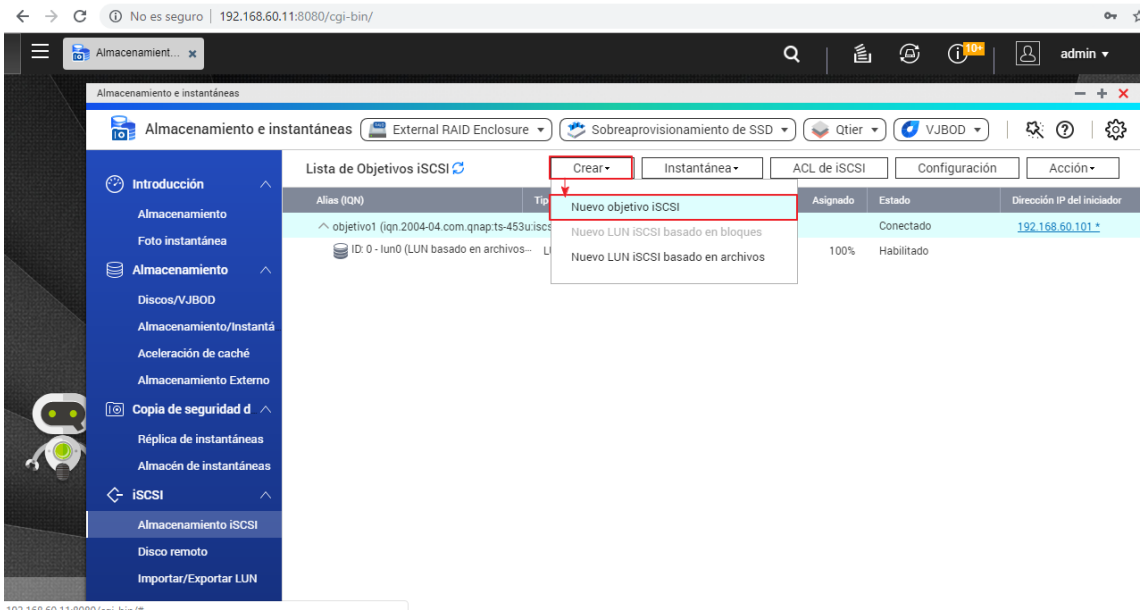


Figura 8.13: Nuevo objetivo *iSCSI*.

Figura 8.14: Asistente de creación de objetivo *iSCSI* y LUN asociado.

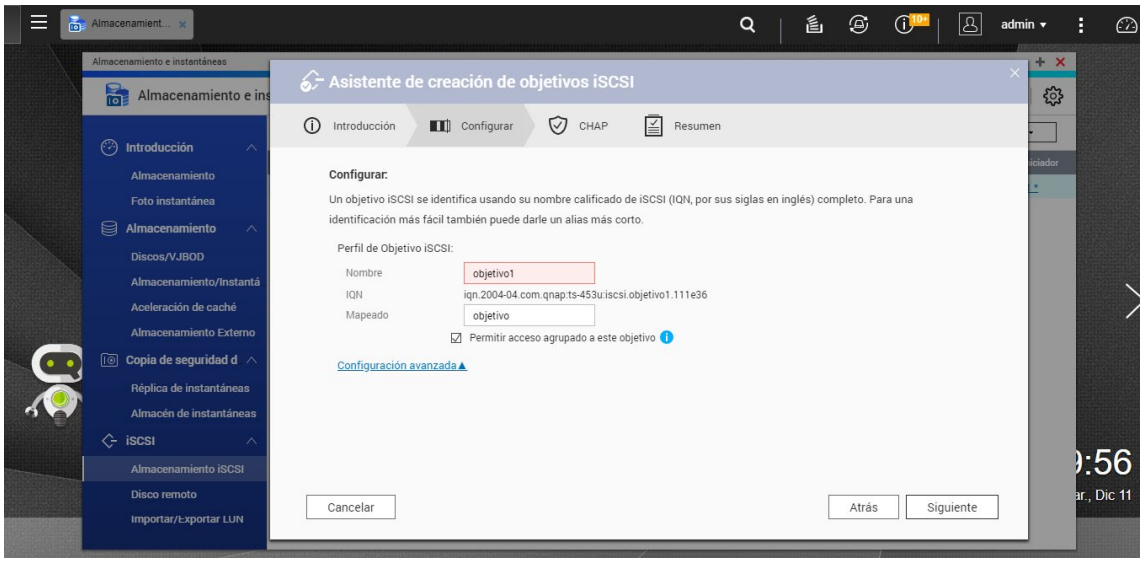


Figura 8.15: Especificación de nombre al objetivo *iSCSI*.

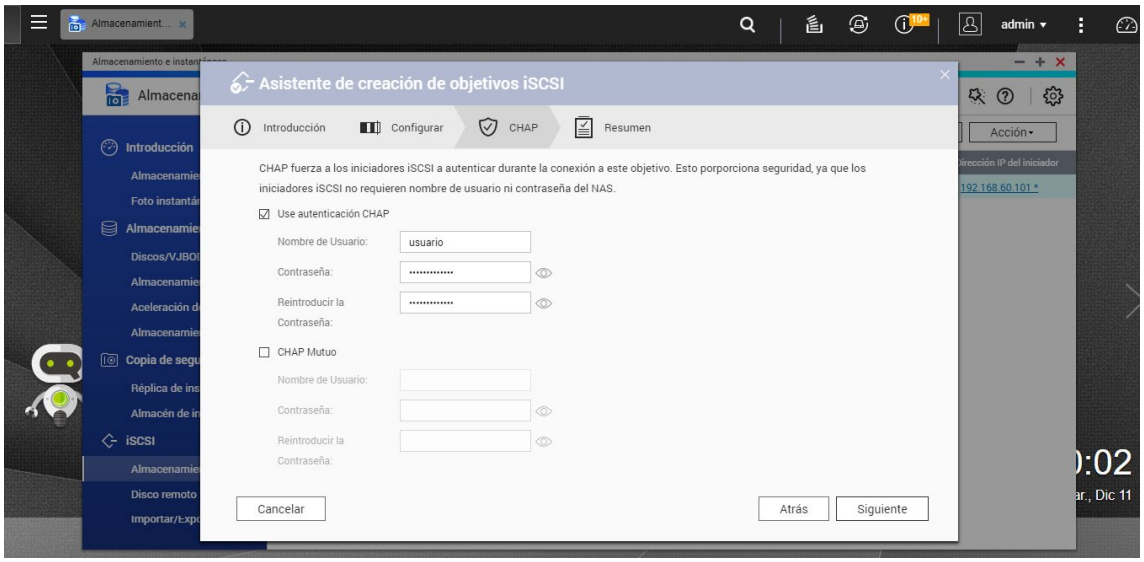


Figura 8.16: Configuración de CHAP.

En la Figura 8.16 se muestra la ventana de configuración de CHAP. Según el nivel de seguridad que se requiera en la red es recomendable configurarlo, incluso de forma mutua. Esta medida de seguridad hace que, para poder conectar al dispositivo de almacenamiento, se deba iniciar sesión con el usuario especificado en la configuración CHAP.

La siguiente ventana muestra un resumen de la configuración. Además, es aquí donde se especifica la creación de un LUN asociado a este objetivo *iSCSI*.

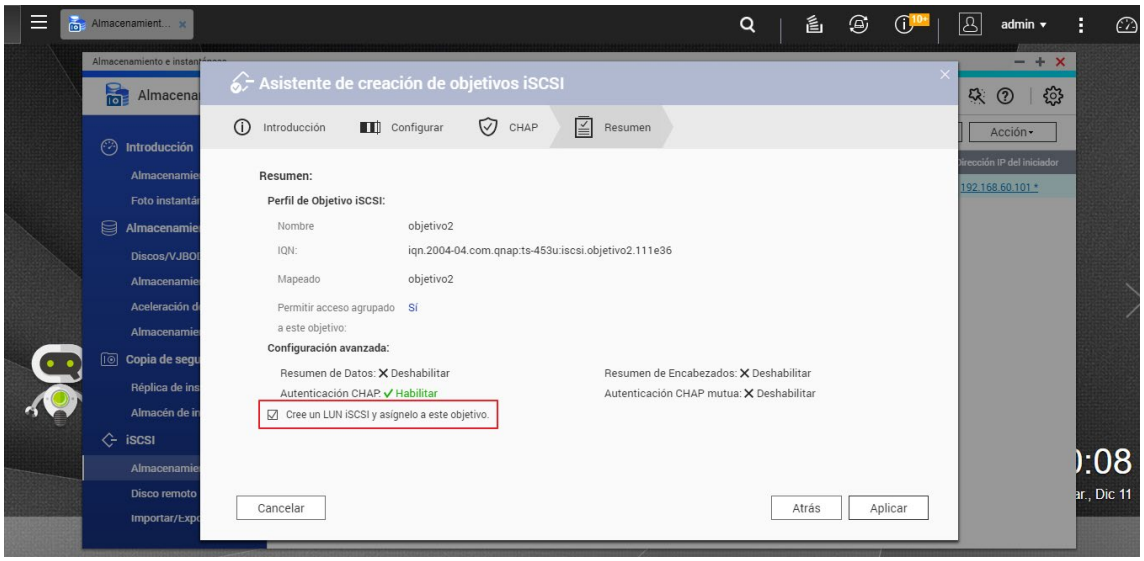


Figura 8.17: Resumen de configuración y creación de LUN asociado.

Hecho esto, el NAS ya está preparado para que los hosts se conecten a él vía iSCSI para tener almacenamiento compartido.

Nota

En entornos de producción TODOS los equipos de almacenamiento (SAN) disponen de redes independientes para almacenamiento (habitualmente Fibre Channel o iSCSI) y para administración/gestión/monitorización.

8.2.3 Hosts de virtualización

Una vez preparado el almacenamiento y el dominio, se puede proceder a la configuración de los servidores físicos de HP, que se utilizarán para ejecutar las VMs tanto del sistema *SCVMM* como las de los clientes de prueba. En ambos hosts se deben seguir los mismos pasos, exceptuando algunos casos, como por ejemplo la IP asignada, donde cada host tendrá una diferente. Lo primero que se hace al iniciar un host nuevo, es acceder al *intelligent provisioning* para configurar los discos locales. Simplemente hay que pulsar la tecla F10 mientras se está iniciando (según la versión puede cambiar la tecla, pero la información aparece en la pantalla tal y como se muestra en la Figura 8.18).

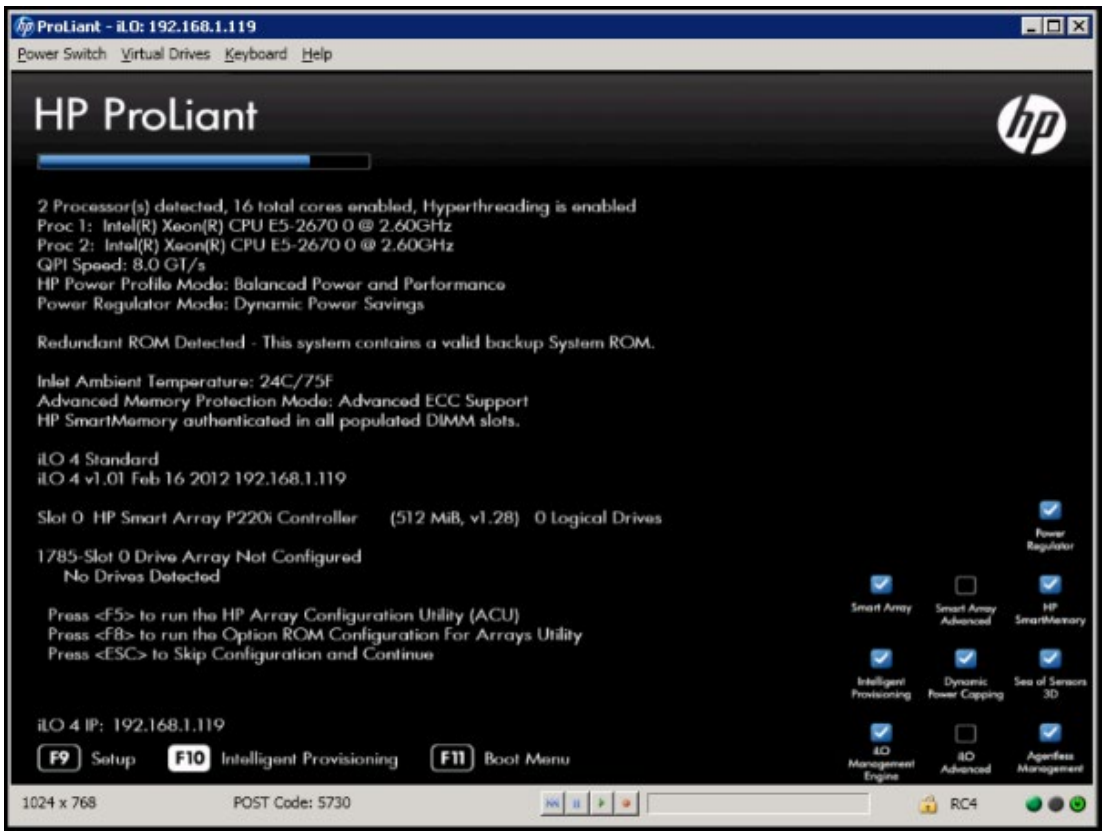


Figura 8.18: Ejemplo de pantalla de inicio de los servidores HP ProLiant.

Una vez se haya accedido a esta opción, se pueden personalizar una serie de parámetros (Hardware, sistema operativo desde el CD de instalación, cuenta de administrador local) y al finalizar se instalará el sistema. Al terminar la instalación, tal y como se ha hecho previamente con el DC, se comprueban las actualizaciones del sistema.

Seguidamente se explicará, en el orden que sigue, la configuración necesaria en los hosts:

i. Preparación y conexión al NAS de almacenamiento mediante *iSCSI*,
ii. Creación y configuración de teams de tarjetas de red para unión al dominio,
iii. Instalación y configuración del rol de clúster de conmutación por error,
iv. Instalación y configuración del rol de Hyper-V.

8.2.3.1 Preparación y conexión del NAS de almacenamiento mediante iSCSI

El siguiente paso es conectar los servidores al NAS. Para ello se debe instalar el rol de *iSCSI*, tal y como se muestra en la Figura 8.19. Es recomendable instalar también las características mencionadas en la sección de configuración del DC.

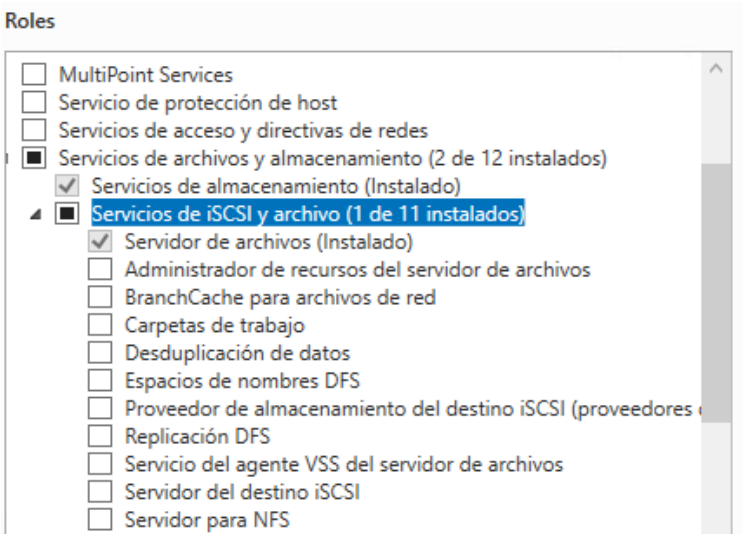


Figura 8.19: rol de *iSCSI*.

Como opción de failover [1], se recomienda tener múltiples caminos de red entre los hosts y la cabina, por lo tanto, será necesario instalar la característica MPIO (Multipath I/O o E/S de múltiples rutas) en dichos hosts, como muestra la Figura 8.20.

[1] Modo de funcionamiento de respaldo en el que las funciones de un componente son asumidos por otros el componente principal no está disponible.

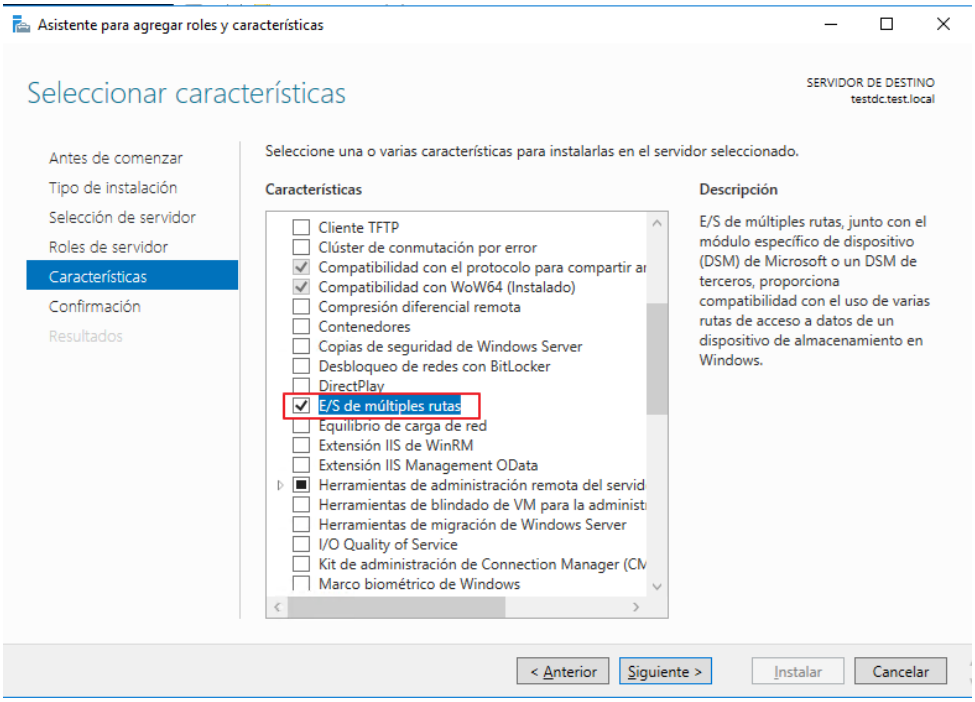


Figura 8.20: Selección de la característica Multipath I/O.

Una vez termine la instalación, se debe acceder a la herramienta *Iniciador iSCSI* que se habrá instalado, y conectar al NAS utilizando la IP que se le ha asignado previamente, en nuestro caso 192.168.60.11, tal y como muestra la Figura 8.21.

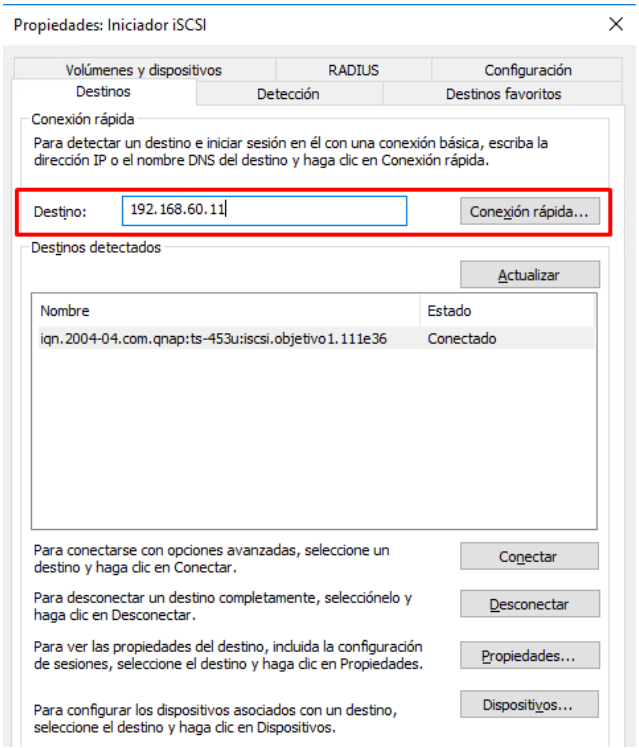


Figura 8.21: Configuración del iniciador *iSCSI*.

8.2.3.2 *Creación y configuración de teams de tarjetas de red para unión al dominio*

El siguiente paso es agregar los hosts de virtualización al dominio creado en el DC. Para ello, se deben realizar configuraciones previas para que todo funcione correctamente. Primero, se crean los teams de tarjetas de red, para lograr redundancia de red tal y como se tiene en el entorno real. Uno de los hosts tiene únicamente dos tarjetas por lo que el team no sería necesario, ya que cada team será de una única tarjeta. Para crearlos, se accede al panel de administrador de servidor local y se habilita la formación de equipos NIC, tal y como muestra la Figura 8.22. Al seleccionar la opción *Deshabilitado/Habilitado* que aparece, se abre una nueva ventana que permite crear los dos teams necesarios: team administración y team hyper-v. El team de administración se utilizará para tráfico de las máquinas de administración, en nuestro caso serán los hosts y las VMs del sistema *SCVMM*. El team de hyper-v se utilizará para el resto de las máquinas virtuales (habitualmente de clientes), de manera que el tráfico vaya por redes separadas físicamente. Para crear un nuevo team se debe pulsar en *Tareas* y agregar un *nuevo equipo,* tal y como muestra la Figura 8.23. Después, se seleccionan los adaptadores de red que formarán parte de ese team.

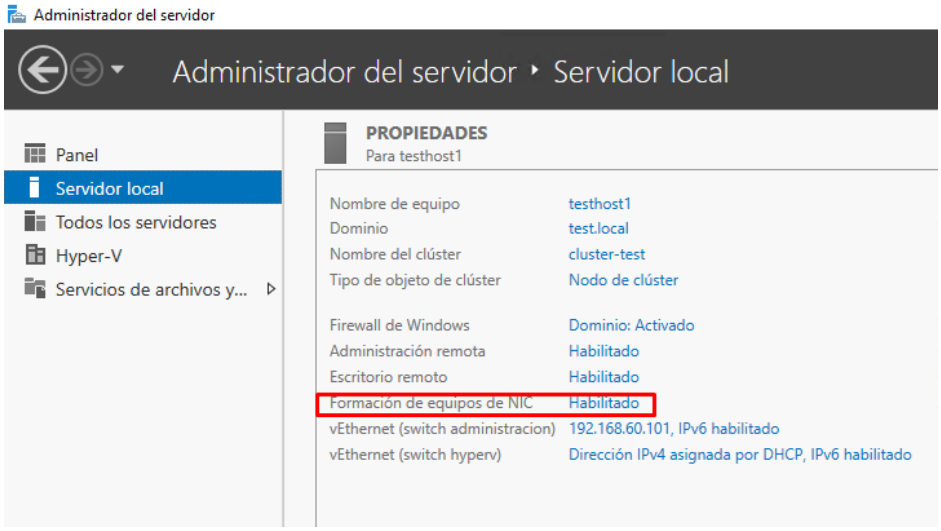


Figura 8.22: Formación de teams.

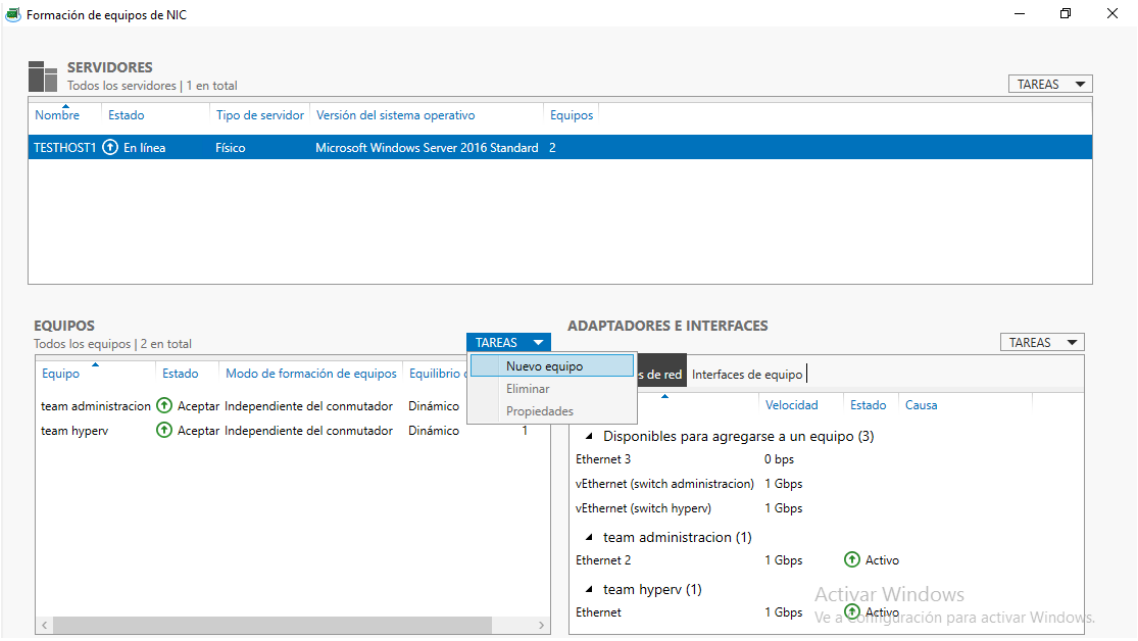


Figura 8.23: creación de nuevo team.

Con los teams creados, solo falta indicar a uno de ellos, en nuestro caso utilizaremos el de administración, que su DNS sea la VM creada al principio, que ejerce de DC y servidor DNS. Para ello, se accede al menú de adaptadores de red tal y como se ha hecho para el DC, y así poder cambiar la configuración. En este caso, solo es necesario modificar la información del DNS, tal y como muestra la Figura 8.24.

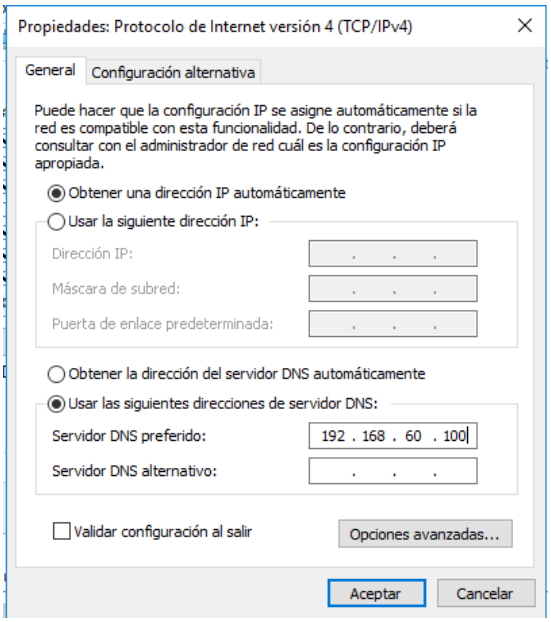


Figura 8.24: Configuración de DNS del team administración.

Seguidamente se pueden unir los equipos al dominio test.local, creado desde el DC anteriormente. Para ello, en el panel de *administrador del servidor*, se debe hacer click en *grupo de trabajo*, que aparece en el mismo lugar que aparece *dominio* en la Figura 8.25. Se abre entonces una nueva ventana, donde se debe seleccionar la opción *Cambiar*

y especificar el nombre del equipo y del dominio al que se unirán los hosts tal y como muestra la Figura 8.26.

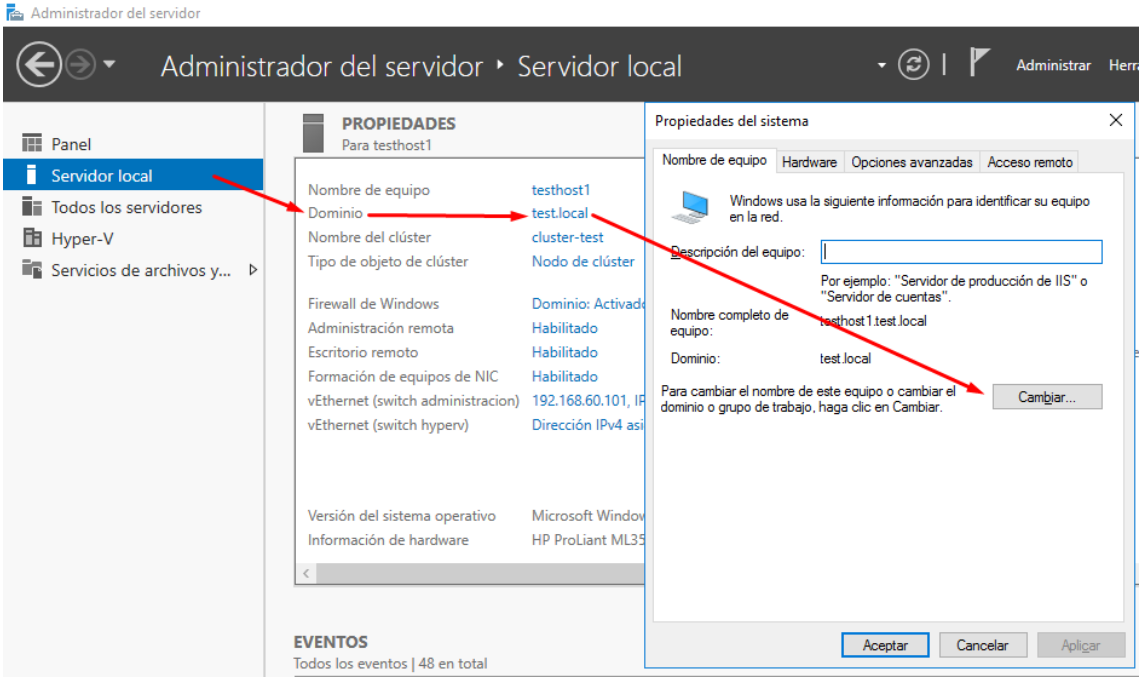


Figura 8.25: Menú de modificación del dominio y nombre del equipo.

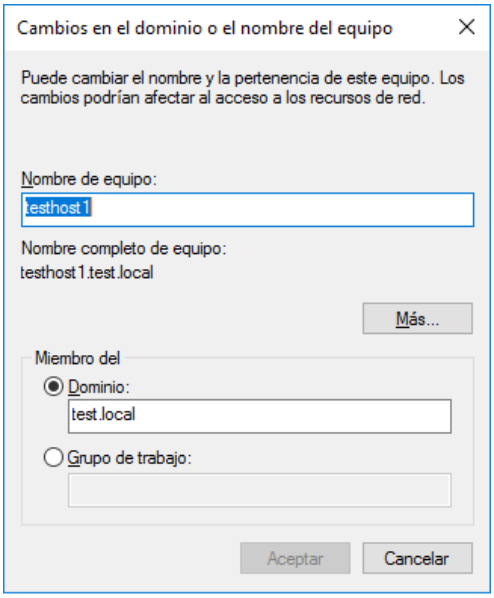


Figura 8.26: modificación del nombre y dominio del equipo.

Los nombres de los hosts serán: testhost1 y testhost2. Ambos se unirán al dominio test.local. Al pulsar *Aceptar*, hay que reiniciar los equipos para que los cambios sean efectivos.

Una vez se hayan reiniciado, iniciamos sesión con el usuario creado previamente en el DC, VMMAdmin. Es momento de configurar el clúster de conmutación por error para que los hosts trabajen de manera conjunta.

8.2.3.3 *Instalación y configuración del rol de clúster de conmutación por error*

Para hacerlo, hay que instalar la característica correspondiente: *clúster de conmutación por error,* que aparece en las características al añadir un nuevo rol, como muestra la Figura 8.27.

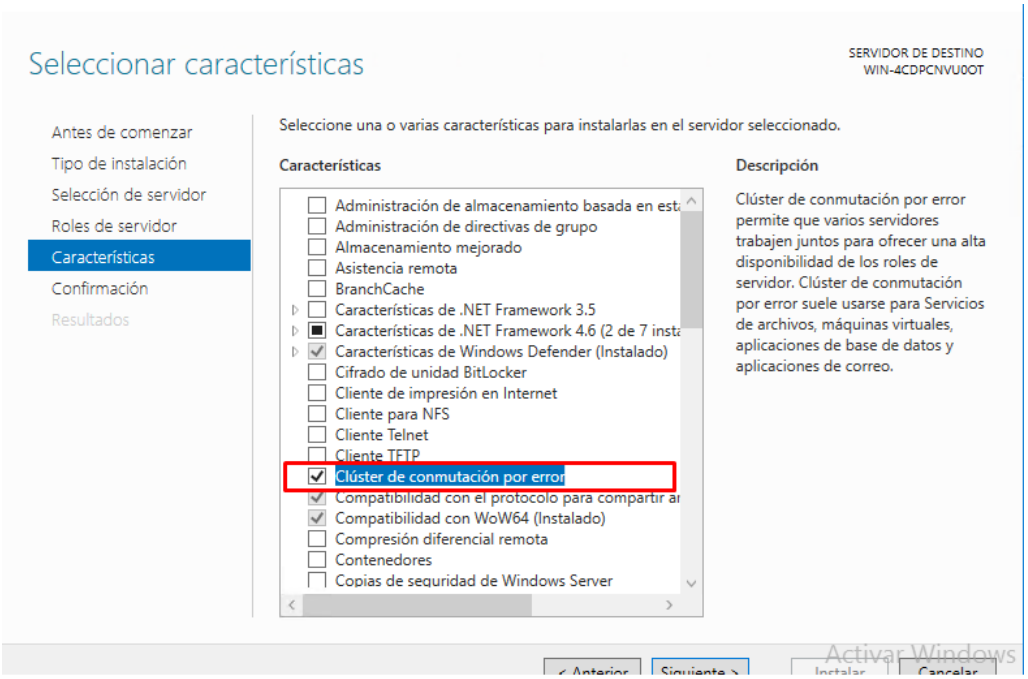


Figura 8.27: instalación del clúster.

Una vez haya acabado la instalación, es momento de crear y configurar el clúster. Para ello, se debe abrir la herramienta de *administración de clústeres de conmutación por error*. Una vez abierta, al pulsar en *Crear clúster* se inicia un asistente para hacer la configuración. En las siguientes secciones, se deben indicar los servidores que formarán parte de este clúster escribiendo los nombres y pulsando *agregar*. Sin embargo, en nuestro caso personal, en testhost2 se instaló la característica con anterioridad. De esta manera se creó el clúster con un único servidor, y el segundo se añadió más tarde. Al pulsar siguiente después de haber añadido el/los servidores, se debe escoger si realizar o no las pruebas de validación, que empezarán a ejecutarse al pulsar *siguiente* en caso de querer realizarlas. Es recomendable realizarlas por si hubiese algún problema con los servidores. Una vez realizadas, se especifican el nombre y la dirección IP del clúster, en nuestro caso se le ha nombrado “cluster-test” y se le ha fijado la IP 192.168.60.103, tal y como muestra la Figura 8.28. El resto de las secciones se debe pulsar siguiente hasta finalizar el asistente de creación.

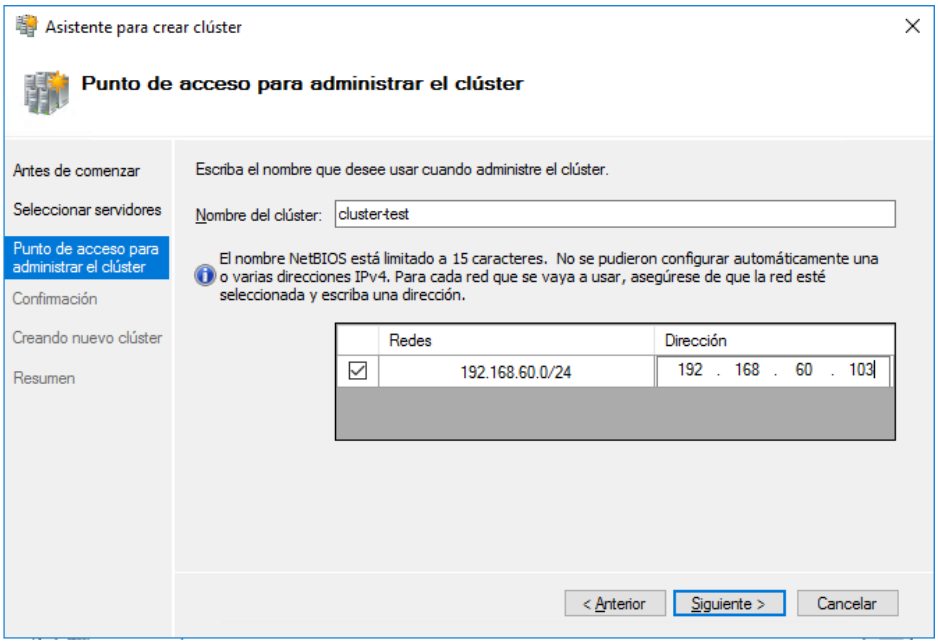


Figura 8.28: nombre y IP del clúster.

Una vez instalado el clúster, se debe añadir el almacenamiento compartido para que los servidores en el clúster lo puedan utilizar. Para hacerlo, desde el *administrador de clúster de conmutación por error*, hay que acceder a la pestaña de discos, y agregar un disco. Se abre una nueva ventana y, si se han realizado los pasos anteriores correctamente (en concreto la configuración del NAS y de *iSCSI*), se verá el volumen disponible, tal y como muestra la Figura 8.29. Para terminar, se debe agregar el nuevo disco a volúmenes compartidos de clúster, tal y como muestra la Figura 8.30.

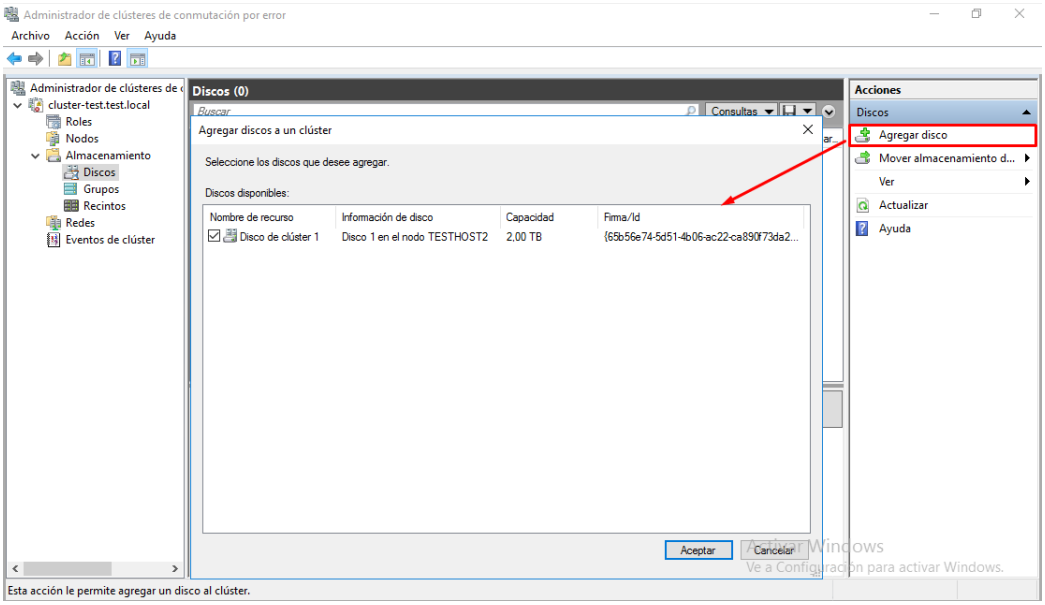


Figura 8.29: Agregar disco de clúster.

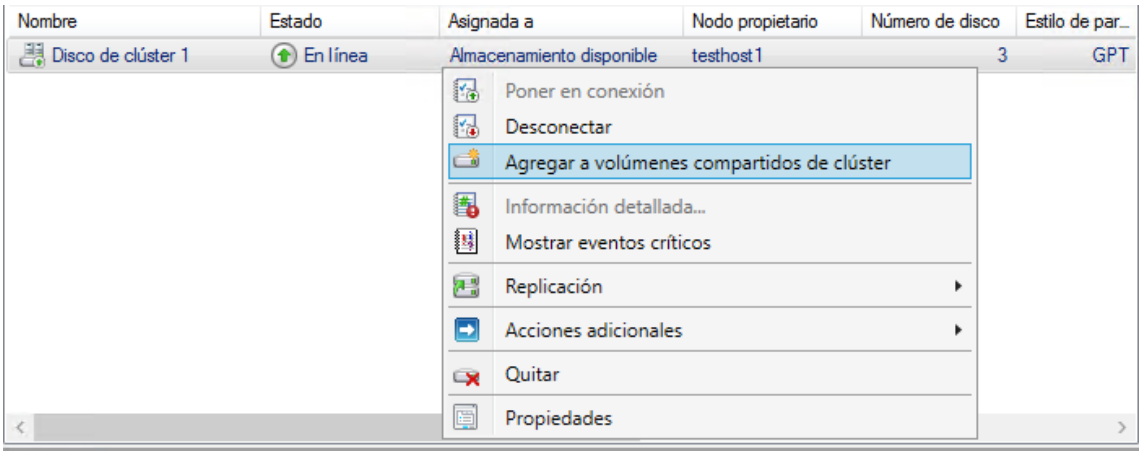


Figura 8.30: Agregar a volúmenes compartidos de clúster.

Por último, queda configurar el quórum de clúster que, explicado en pocos términos, sirve que los todos los hosts del clúster trabajen de forma controlada y que ninguno tome posesión o intente proporcionar un servicio para el cual no está autorizado en cada momento. El objetivo del quórum es mejorar la disponibilidad del clúster, para simplificar la decisión de escoger un nodo en el momento de migrar las VMs.

Existen dos tipos de quórum: LUN exclusiva para quórum, o recurso de red compartido de quórum (por simplicidad se ha escogido el segundo). Para configurarlo, primero se debe crear el recurso compartido mediante el cual los servidores se comunicarán. Este recurso se ha ubicado en la VM del DC y es una carpeta a la que se ha nombrado *quorum*.

Para que los hosts puedan utilizarla como recurso compartido, se les debe permitir el acceso. Para ello, se deben abrir las propiedades de la carpeta, haciendo click derecho sobre ella. En la pestaña *Seguridad*, se debe pulsar en *Editar* para agregar los hosts de virtualización. Luego, se debe pulsar en *Agregar*, y la manera más sencilla de buscar los hosts es utilizando las *opciones avanzadas*. En este punto se debe comprobar que *Equipos* está seleccionado en *Tipos de objeto* antes de pulsar en *Buscar ahora*. Al hacerlo aparece una lista de usuarios y equipos del dominio, donde se pueden seleccionar los hosts de uno en uno haciendo doble click sobre ellos, o seleccionándolos y pulsando *aceptar*. Una vez agregados, se les debe ofrecer permisos de control total. Este proceso se detalla en las Figuras 8.31 y 8.32.

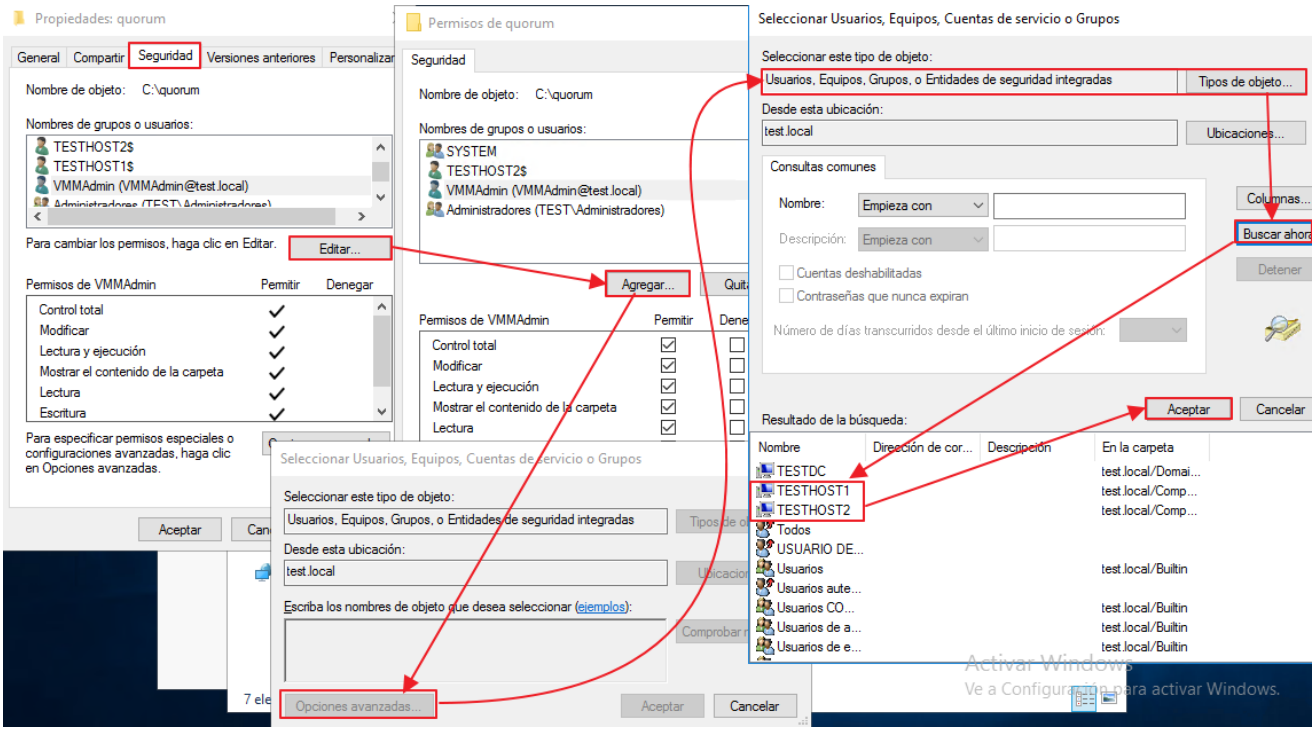


Figura 8.31: Agregación de los hosts en la seguridad de la carpeta de quórum.

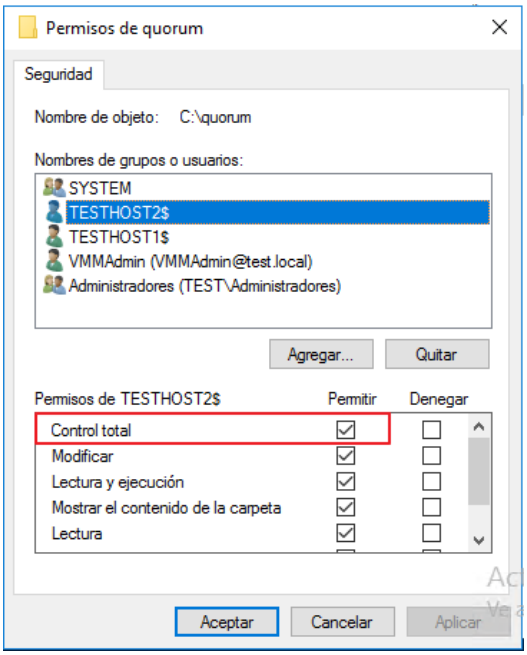


Figura 8.32: Permisos de los hosts sobre la carpeta quórum.

Una vez agregados los hosts, el recurso está preparado para configurarlo en el administrador de clúster de conmutación por error. Para ello, se debe abrir la configuración del quórum como muestra la Figura 8.33.

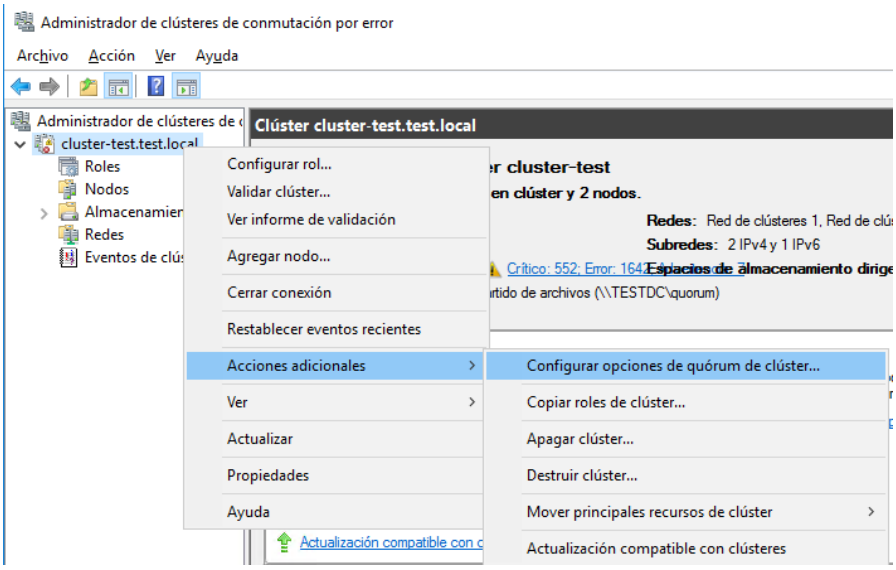


Figura 8.33: Configuración del quórum de clúster.

Se abre un asistente, en el cual se han escogido las siguientes opciones:

i. Seleccionar el testigo de quórum.
ii. Configurar un testigo de recurso compartido de archivos.
iii. Ruta de acceso de recurso compartido: \\nombre del DC*carpetacreada* (en nuestro caso la hemos creado en la carpeta C, si no se hubiese hecho así, habría que poner la ruta completa p.ej. \\nombre\Documentos\carpeta).

Los siguientes pasos se pueden dejar con las opciones por defecto.
Falta por tanto unir el segundo servidor al clúster, en el que no es necesario realizar la configuración del quórum ni del almacenamiento compartido. Para unirlo, en lugar de seleccionar la opción *Crear* en el *administrador de clúster de conmutación por error*, se debe seleccionar *Conectar al clúster*. Se abre entonces una ventana en la que se debe escribir el nombre del clúster recientemente creado, "cluster-test", y finalmente aceptar.

8.2.3.4 Instalación y configuración de Hyper-V

El último paso en los servidores físicos es instalar el rol de Hyper-V para poder crear las VMs que ejecutarán el sistema *SCVMM*. Para ello, se debe agregar el rol de Hyper-v mediante el *administrador del servidor* en ambos servidores. Las opciones que aparecen deben dejarse por defecto excepto la configuración de conmutadores virtuales, momento en que se pide qué conmutador se utilizará para administrar las VM. Se debe seleccionar entonces el team hyper-v previamente creado, tal y como muestra la Figura 8.34. Una vez instalado, se debe configurar este conmutador virtual para uso exclusivo de Hyper-V y así evitar conflictos entre el sistema operativo host y las VMs. Para ello hay que acceder al administrador de Hyper-V, y entrar a la configuración de conmutadores virtuales, tal y como se muestra en la Figura 8.35. Se abre entonces una nueva ventana, donde se puede observar el conmutador virtual. Es recomendable modificar el nombre, y fijar el mismo en ambos hosts, ya que en caso contrario puede haber problemas en la comunicación de las VM entre hosts (p.ej al migrar una VM de un host a otro, no se

detectará el mismo conmutador y fallará la migración). En esta sección es también donde puede establecerse que el conmutador virtual es de uso exclusivo para Hyper-V. Se puede también crear el conmutador virtual para el team administración, tal y como muestra la Figura 8.36.

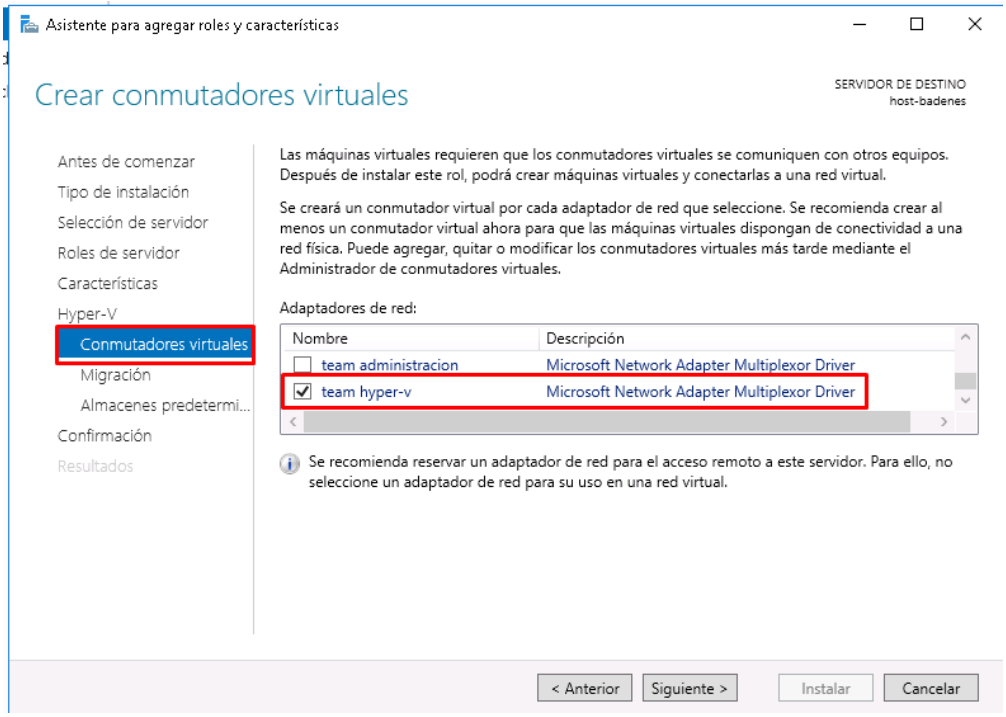


Figura 8.34: Selección del team para Hyper-V.

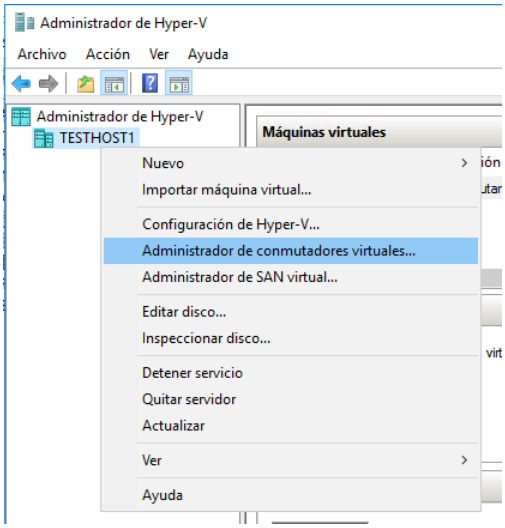


Figura 8.35: Administrador de conmutadores virtuales.

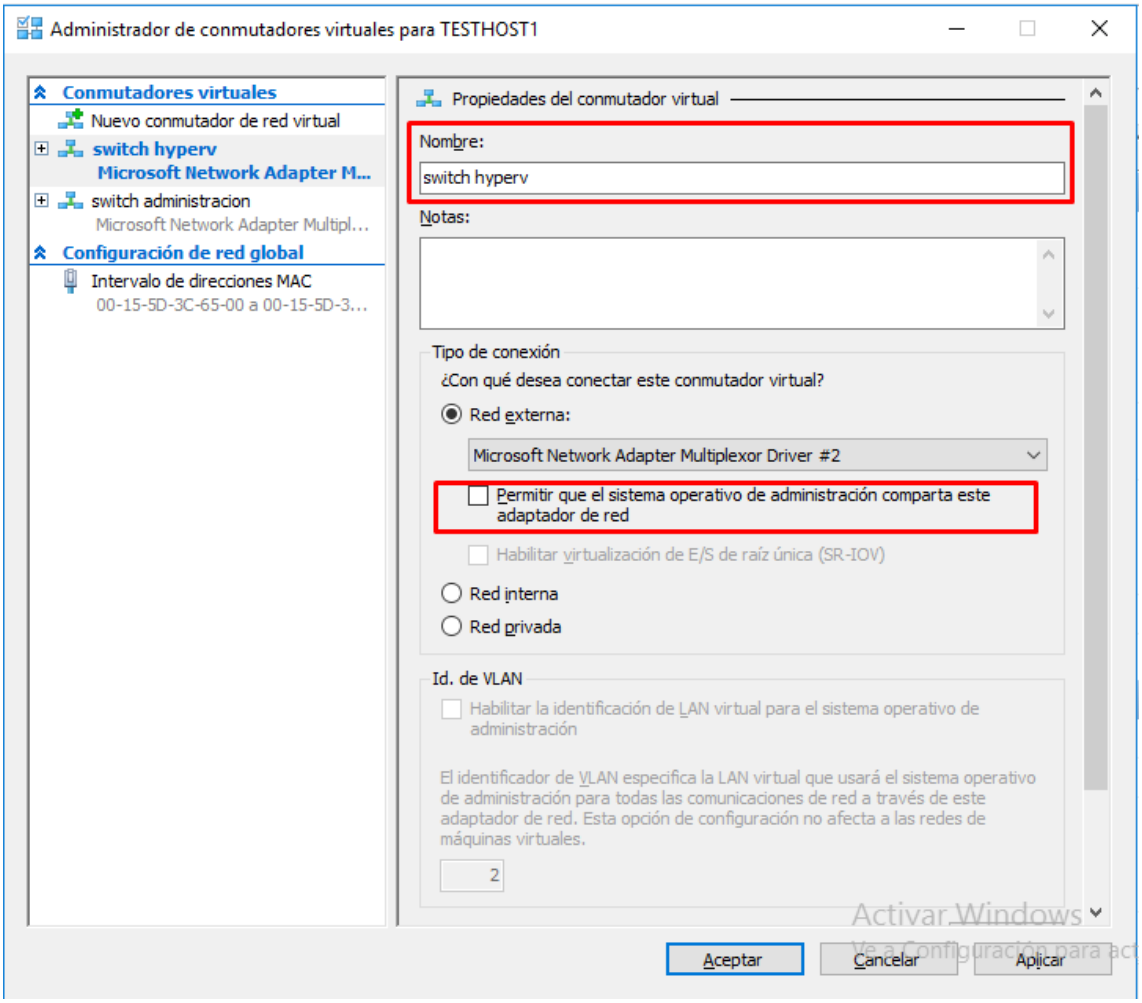


Figura 8.36: Nombre y exclusividad del conmutador virtual.

Una vez configurados los conmutadores virtuales, se pueden crear las VMs para poder instalar el sistema *SCVMM*.

8.3 Preparación del entorno virtual

En esta sección se explicará en detalle qué VMs hacen falta, cómo crearlas y prepararlas para poder instalar el sistema *SCVMM* y, por último, la instalación del sistema.

8.3.1 Creación de la primera VM

Para crear todas las VMs de manera relativamente rápida, primero se prepara una VM con una configuración básica y así utilizarla como base para crear el resto. El primer paso por tanto es crear una VM con el sistema operativo Windows Server 2016 Standard con experiencia de escritorio, e instalar todas las actualizaciones que haya disponibles. Para crearla, se pueden seguir los pasos descritos para la creación de la VM del DC hasta llegar al punto de instalar las actualizaciones. A esta VM la nombraremos libvmm, por ejemplo, y se han establecido los siguientes valores, basándonos en los requisitos de hardware:

i. Procesadores: 2 procesadores virtuales.
ii. Memoria RAM: 2048 MB.
iii. Red: conectado a switch administración.

Los discos de las VMs que creemos a partir de este punto, sin embargo, irán ubicados en el almacenamiento compartido de clúster:

i. Ubicación de la configuración de la VM: C:\ClústerStorage\Volume1\HyperV.
ii. Ubicación del disco de la VM: C:\ClústerStorage\Volume1\HyperV\VHD.

8.3.2 Preparación del resto de VMs

Tal y como se muestra en el estudio de requisitos, son necesarias varias VMs:

i. Servidor *VMM.*
ii. Base de datos.
iii. Librería.
iv. Consola *VMM.*

La consola y librería se instalan por defecto junto con el servidor en la misma máquina. Sin embargo, es interesante poder instalar una librería y consola remotas, por si fallase la VM de servidor, no perder todos los datos.

Lo primero que se debe hacer, es preparar el disco para poder utilizarlo para las demás máquinas. Para ello se ejecuta sysprep, que prepara el sistema para que, al reiniciar el equipo vuelva a establecer el identificador universal de la máquina, indicar otra licencia, etc., como si el sistema operativo se hubiese instalado de nuevo. Para hacerlo, se accede a C:\Windows\System32\Sysprep y se ejecuta el programa *sysprep.exe*. Se abre entonces la interfaz del programa, en la cual se marca la opción *generalizar* con la opción de *apagar* antes de aceptar, tal y como muestra la Figura 8.37.

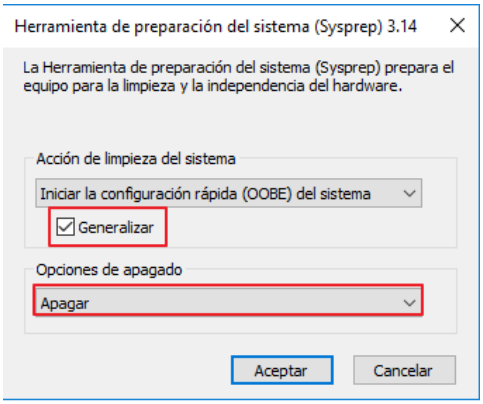


Figura 8.37: Herramienta sysprep.

Una vez hecho, se pueden crear las VMs utilizando la creada anteriormente como plantilla. Para hacerlo, una forma rápida de hacerlo es copiar y pegar el disco de la VM, de manera que queden cuatro discos en total, uno por cada VM. Después se crean las tres VMs restantes, y en lugar de crear un disco nuevo, se utiliza uno existente, tal y

como muestra la Figura 8.38. En la configuración de red, se selecciona el switch de administración, creado anteriormente, después de instalar Hyper-V.

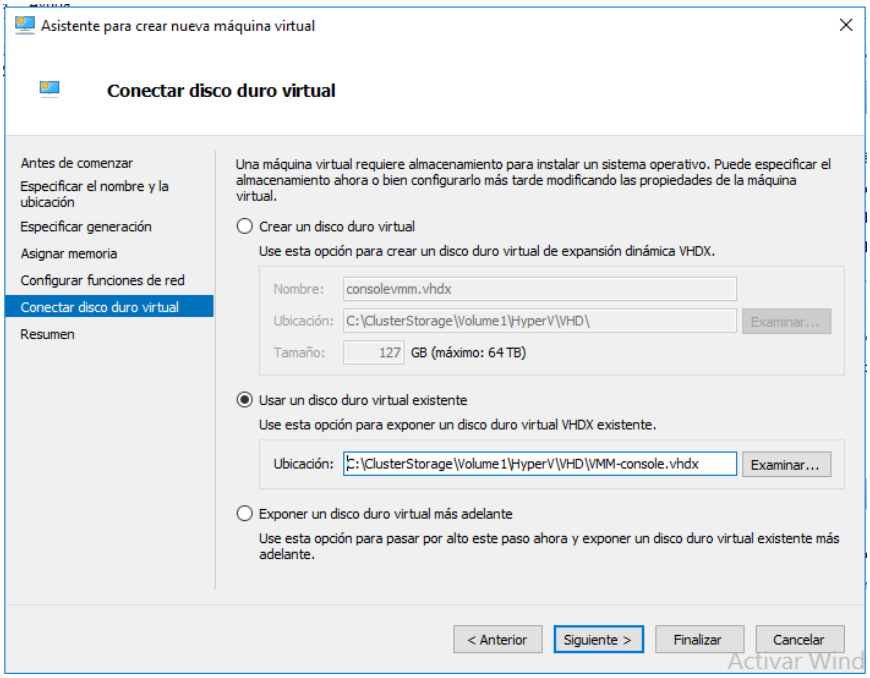


Figura 8.38: Uso de un disco existente.

Una vez creadas, no se debe instalar ningún sistema operativo, ya que en los discos ya está instalado. Antes de preparar los componentes necesarios para *SCVMM* en cada máquina, es recomendable fijar una IP para cada VM y posteriormente unirlas al dominio *test*. En nuestro caso, se han fijado estas IPs como sigue:

i. Servidor *VMM*: 192.168.60.104.
ii. Base de datos: 192.168.60.106.
iii. Librería *VMM*: 192.168.60.105.
iv. Consola *VMM*: 192.168.60.107.

8.3.2.1 Base de datos

La primera máquina preparada ha sido la de la base de datos. La base de datos de *VMM* almacena toda la información de configuración de *VMM*. La versión de SQL instalada es SQL Server 2016, que como se especifica en el estudio de requisitos, es compatible con la versión de *SCVMM* 2016. Para hacerlo, se ejecuta el archivo de instalación de SQL Server y se continua con las opciones por defecto excepto en el aprovisionamiento de cuentas, donde se debe agregar el usuario actual (para poder conectar con permisos de administrador a la base de datos y realizar las configuraciones pertinentes) y en la selección de características, donde hay que escoger las siguientes:

i. Servicios de motor de base de datos.
ii. Conectividad con las herramientas de cliente.
iii. Compatibilidad con versiones anteriores de las herramientas.
iv. SDK de conectividad de cliente SQL.

Cabe destacar que para *VMM* únicamente es necesario instalar los servicios de motor de base de datos, sin embargo, para poder utilizar otros servicios, pueden ser útiles las demás.

En versiones anteriores de SQL Server, al realizar esta instalación se incluían las herramientas de administración. Sin embargo, en la versión de SQL Server 2016, éstas no vienen incluidas y por tanto se deben instalar manualmente. Para hacerlo simplemente se descarga la versión actual desde la página de Microsoft y se ejecuta el archivo de instalación. Una vez instalado, se pueden abrir abrir las herramientas administrativas de SQL (Microsoft SQL Management Studio) para realizar algunas configuraciones necesarias para poder conectar el sistema *SCVMM* a la base de datos:

i. Habilitar las conexiones remotas (ver Figura 8.42).
ii. Configurar SQL para recibir peticiones por un puerto estático.
iii. Permitir tráfico a través del puerto habilitado para SQL.

Una vez abiertas las herramientas administrativas, hay que conectar a la base de datos, tal y como muestra la Figura 8.39.

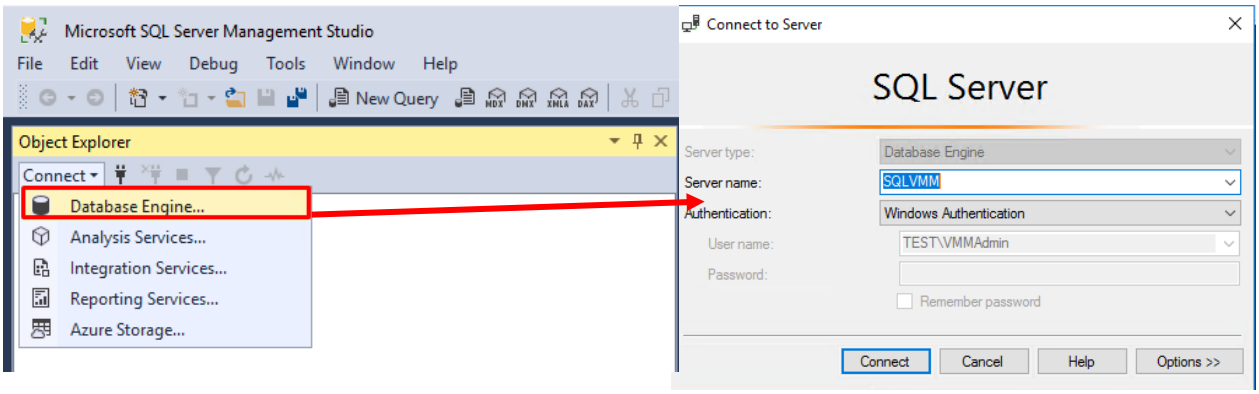


Figura 8.39: conexión a SQL Server.

Una vez realizada la conexión, es recomendable revisar los permisos del usuario VMMAdmin, como se ve en la Figura 8.40.

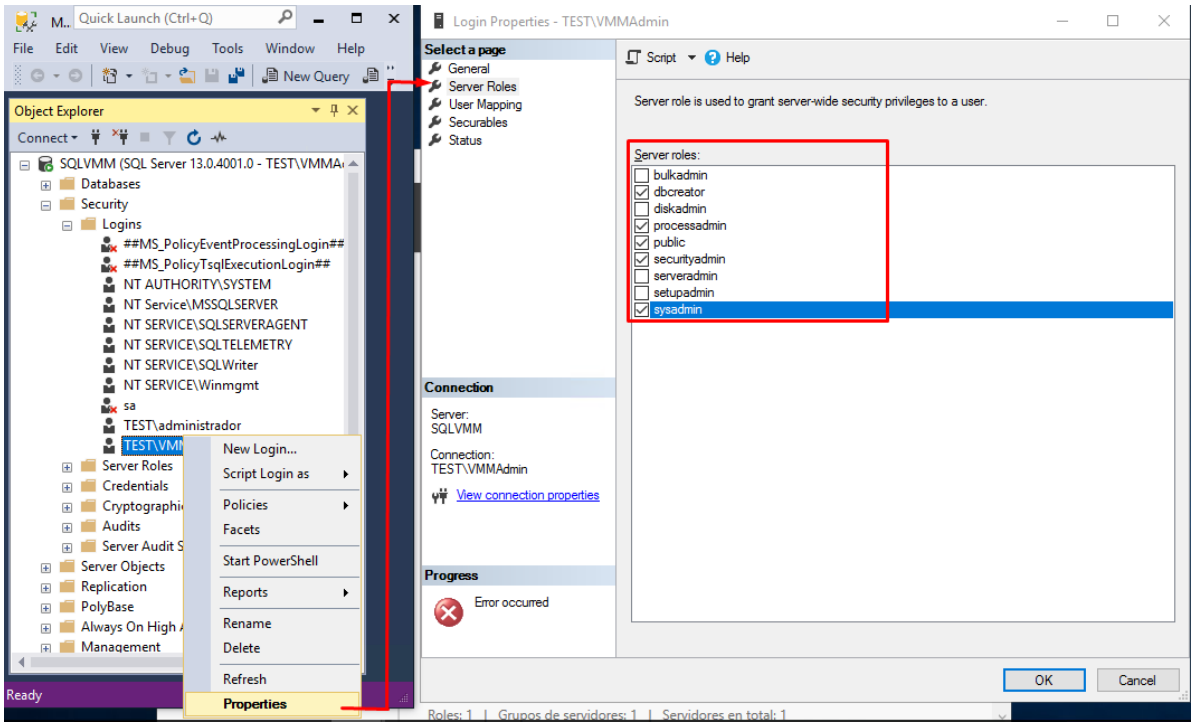


Figura 8.40: Permisos del usuario VMMAdmin.

Si sucede como en nuestro caso, que se instaló desde un usuario del dominio distinto de VMMAdmin, y por tanto la cuenta agregada al instalar SQL Server era test\administrador, se debe acceder desde el usuario que tiene los permisos, y crear un nuevo login para VMMAdmin. Para hacerlo, hay que conectarse igual que en los pasos anteriores, habiendo iniciado sesión con la cuenta test\administrador, hay que seleccionar *New Login* en lugar de *propiedades*, haciendo click derecho en cualquiera de los logins que aparecen en la Figura 8.40. Al hacerlo, se abre una nueva ventana donde se debe especificar el usuario, pulsando la opción *search*, y escribiendo el usuario completo que se quiere añadir (test\VMMAdmin), como muestra la Figura 8.41. Una vez escrito, si se ha hecho correctamente, pulsando en *comprobar nombres* debería aparecer subrayado y con el siguiente formato: usuario (ususario@dominio). Por último, antes de finalizar la creación del login, se debe acceder a la pestaña de permisos, y asignarle los especificados anteriormente. Una vez terminado, ya se puede iniciar sesión con el usuario VMMAdmin y continuar con las configuraciones.

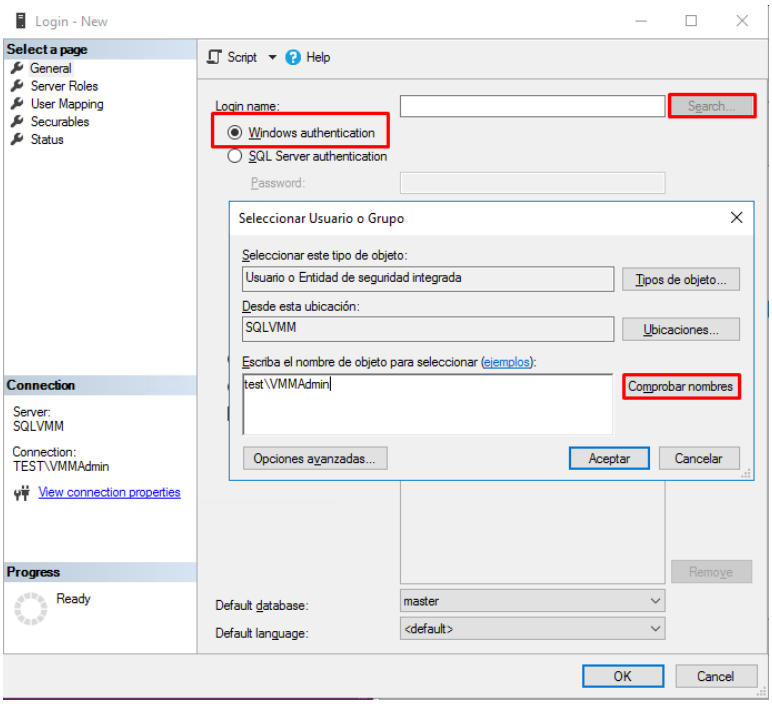


Figura 8.41: creación de nuevo login.

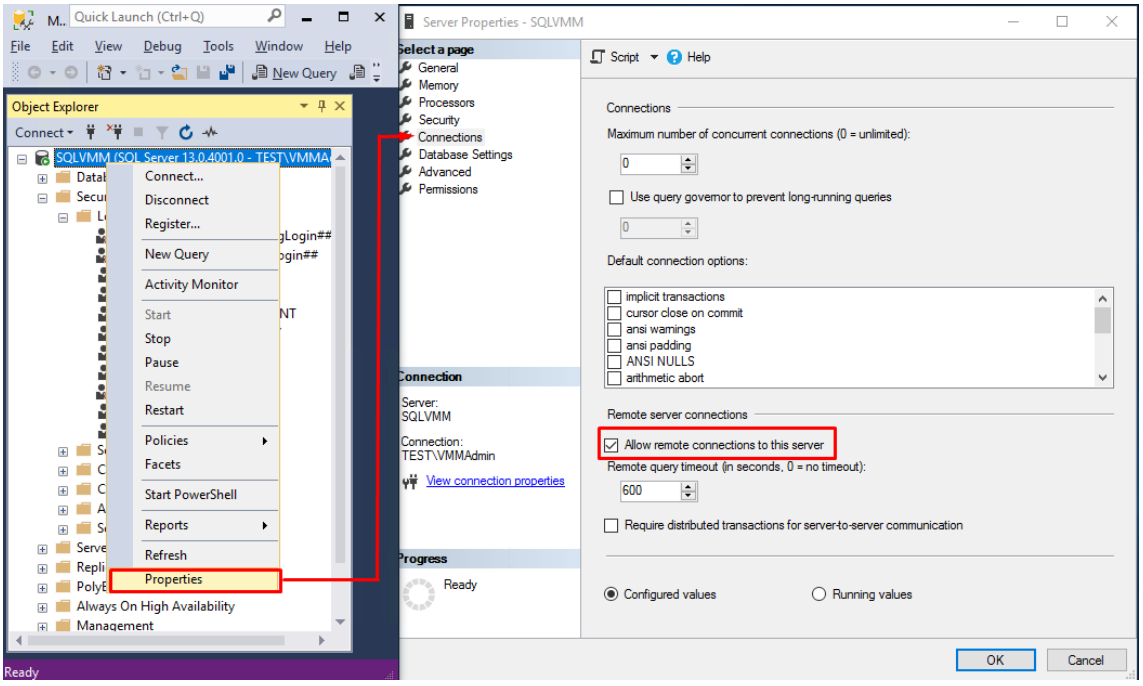


Figura 8.42: Habilitar las conexiones remotas.

En muchos casos la instalación del Servidor SQL se realizará como instancia adicional. Para estos casos es necesario configurar SQL para recibir peticiones por un puerto estático.

Por defecto, el protocolo TCP/IP está deshabilitado, y por lo tanto, hay que habilitarlo. Para ello, se accede al *administrador de configuración de SQL Server 2016* y acceder a la *configuración de red de SQL Server.* Desde este punto, se puede habilitar TCP/IP, tal y como muestra la Figura 8.43. Una vez habilitado, se reinicia el servicio SQL Server (ver Figura 8.44).

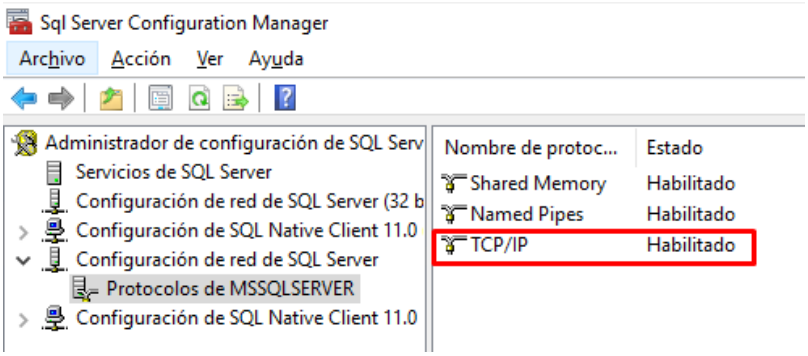


Figura 8.43: Habilitar TCP/IP.

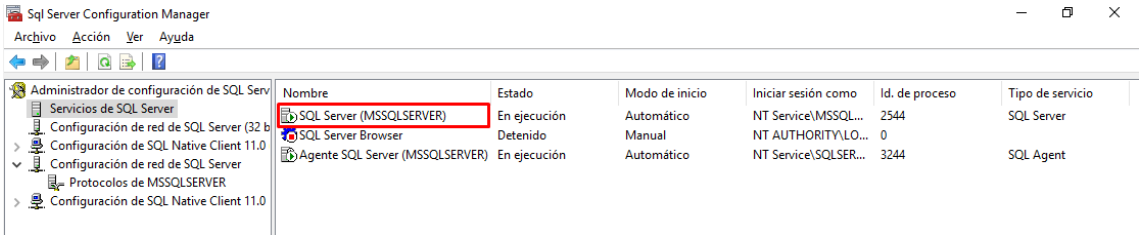


Figura 8.44: Reiniciar el servicio SQL Server.

Por último, para establecer el puerto estático, hay que acceder a las propiedades del protocolo TCP/IP en la configuración de red de SQL Server, acceder a la pestaña direcciones IP, y establecer el puerto TCP, dejando en blanco el puerto TCP dinámico, tal y como se muestra en la Figura 8.45.

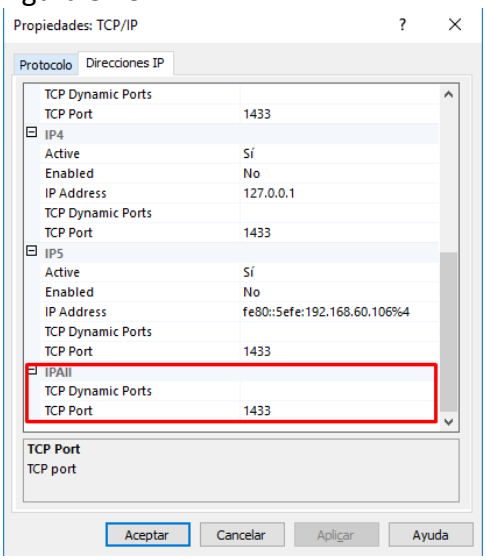


Figura 8.45: Establecer puerto estático.

Una vez habilitado y conociendo el puerto, se debe permitir tráfico a través de este puerto. Para hacerlo, se puede o bien deshabilitar el Firewall completamente, o configurar excepciones para permitir el tráfico. En nuestro caso se ha decidido configurar las excepciones, ya que así se ofrece mayor seguridad. Se deben agregar cuatro excepciones al Firewall de Windows, accediendo a la configuración avanzada y creando nuevas reglas de entrada:

1. Excepción para el puerto TCP 1433: en el asistente al crear nueva regla seleccionar:
   i. Puerto.
   ii. TCP y especificar el puerto 1433.
   iii. Permitir la conexión.
   iv. Seleccionar perfil dominio.
   v. Nombrar la regla, por ejemplo, SQL-TCP 1433.
2. Excepción para el puerto UDP 1434: en el asistente seleccionar:
   i. Puerto.
   ii. UDP y especificar el puerto 1434.
   iii. Permitir la conexión.
   iv. Seleccionar perfil dominio.
   v. Nombrar la regla, por ejemplo, SQL-UDP 1434.
3. Excepción de programa para sqlservr.exe: en el asistente seleccionar:
   i. Programa.
   ii. Seleccionar el programa sqlservr.exe en la ubicación C:\Program Files\MicrosoftSQL Server\MSSQL11.”Nombredeinstancia”\MSSQL\Binn
   iii. Permitir la conexión.
   iv. Seleccionar perfil dominio.
   v. Nombrar la regla, por ejemplo, SQL-sqlservr.exe.
4. Excepción de programa para sqlbrowser.exe: en el asistente seleccionar:
   i. Programa.
   ii. Seleccionar el programa sqlbrowser.exe en la ubicación C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe.
   iii. Permitir la conexión.
   iv. Seleccionar perfil dominio.
   v. Nombrar la regla, por ejemplo, SQL-sqlbrowser.exe.

La VM de la base de datos quedaría con esto configurada. Las VMs de librería y consola no requieren ninguna configuración previa, por lo que a continuación se explicará la configuración necesaria para la instalación de *SCVMM* en la VM servidor *VMM*.

8.3.2.2 Servidor VMM

Como indican los requisitos del sistema, los componentes necesarios para instalar *VMM* en la VM de servidor de *VMM* son:

i. Windows Assestment and Deployment Kit (ADK).
ii. Powershell 5.0.
iii. .NET Framework 4.6.

Si se han seguido correctamente los pasos, únicamente quedaría instalar windows ADK. Para instalarlo, se descarga el archivo de instalación desde la página de Microsoft (https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install) y se ejecuta para instalarlo, muestra la Figura 8.46.

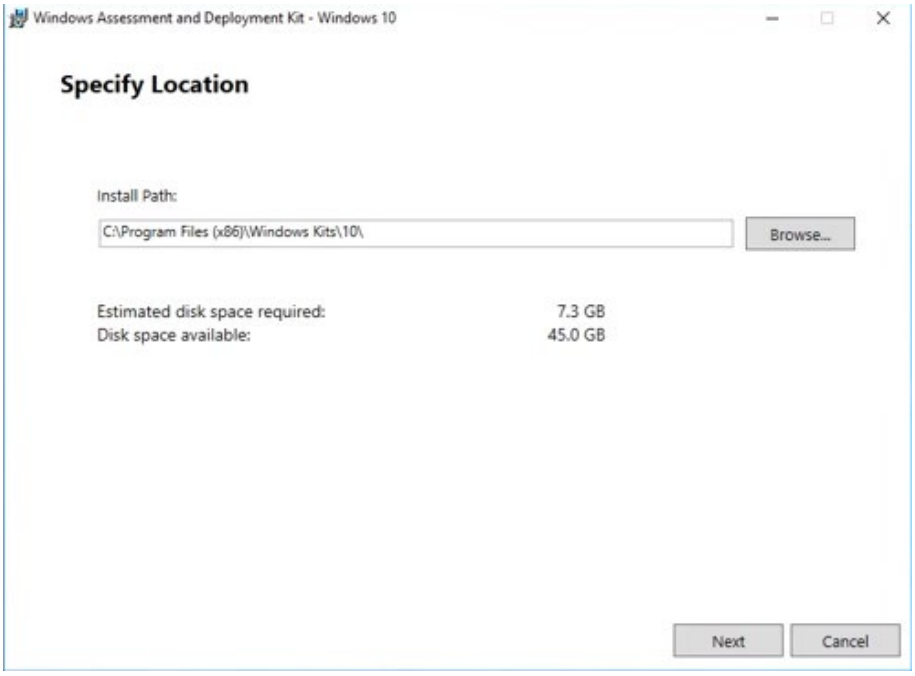


Figura 8.46: Asistente de instalación de Windows ADK.

En la ventana de selección de características, únicamente dos de ellas son necesarias, tal y como indican los requisitos (COMPROBAR SI ESTA LA IMAGEN COMPONENTE-DETALLES):

i. Herramientas de implementación.
ii. Entorno de preinstalación de Windows.

Una vez instalado, se puede instalar *System Center Virtual Machine Manager*, ejecutando el instalador que abre un asistente de instalación, como muestra la Figura 8.47. Para el entorno de pruebas, se ha utilizado la versión de evaluación.

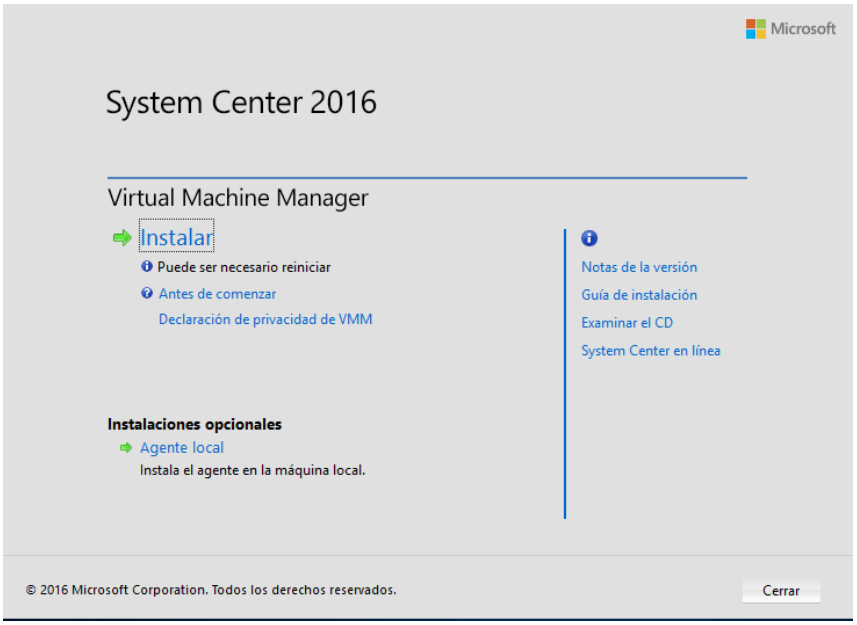


Figura 8.47: Asistente de instalación de *VMM*.

Al pulsar instalar se puede seleccionar que componente se quiere instalar: *Servidor de administración de VMM* o *Consola VMM*. Sin embargo, seleccionando la primera opción, se instala automáticamente la consola. Para esta VM se selecciona *Servidor de administración VMM*. En la información de registro, no se utiliza ninguna clave de producto, para poder así utilizar la versión de evaluación durante 180 días. Las opciones hasta la configuración de la base de datos se pueden dejar por defecto para este entorno.

En el momento de configurar la base de datos, se debe conectar a la VM de SQL configurada anteriormente:

i. Nombre de servidor: se debe utilizar el nombre de equipo de la VM de SQL, en nuestro caso SQLVMM.
ii. Puerto: hay que establecer el puerto que se ha configurado anteriormente, en nuestro caso 1433.
iii. Nombre de usuario y contraseña: usuario administrador de la base de datos, en nuestro caso es el mismo que administra *VMM*, por lo que utilizaremos test\VMMAdmin.
iv. Nombre de instancia y Base de datos: se pueden dejar por defecto.

En el siguiente paso, se debe escoger una cuenta de servicio de *VMM*, en la que se debe especificar test\VMMAdmin, y si se desea utilizar la administración de claves distribuida, que permiten una alta disponibilidad de *VMM*. De forma predeterminada, *VMM* cifra algunos datos en la base de datos de *VMM*. Así, se almacenan algunas credenciales de *VMM* y la información de las claves de productos en el equipo en el que está instalado *VMM* y a la cuenta de servicio utilizada por *VMM* (la cuenta utilizada en la instalación). Esto provoca que, si se mueve la instalación de *VMM* a otro equipo, no se conservan los datos cifrados y hay que especificarlos manualmente. Para asegurar que se conserven,

se debe usar la administración de claves distribuidas para almacenarlas en Active Directory.

Para esto, debe realizarse alguna configuración antes de continuar con la instalación. Hay que crear un contenedor en el dominio para el almacenamiento de las claves. Para hacerlo, se accede a la VM de DC y abrir el editor ADSI. Una vez abierto, hay que conectarse, tal y como muestra la Figura 8.48, y dejar las opciones que aparecen por defecto. A continuación, se crea un nuevo objeto contenedor al que se puede nombrar, por ejemplo, *VMM*.

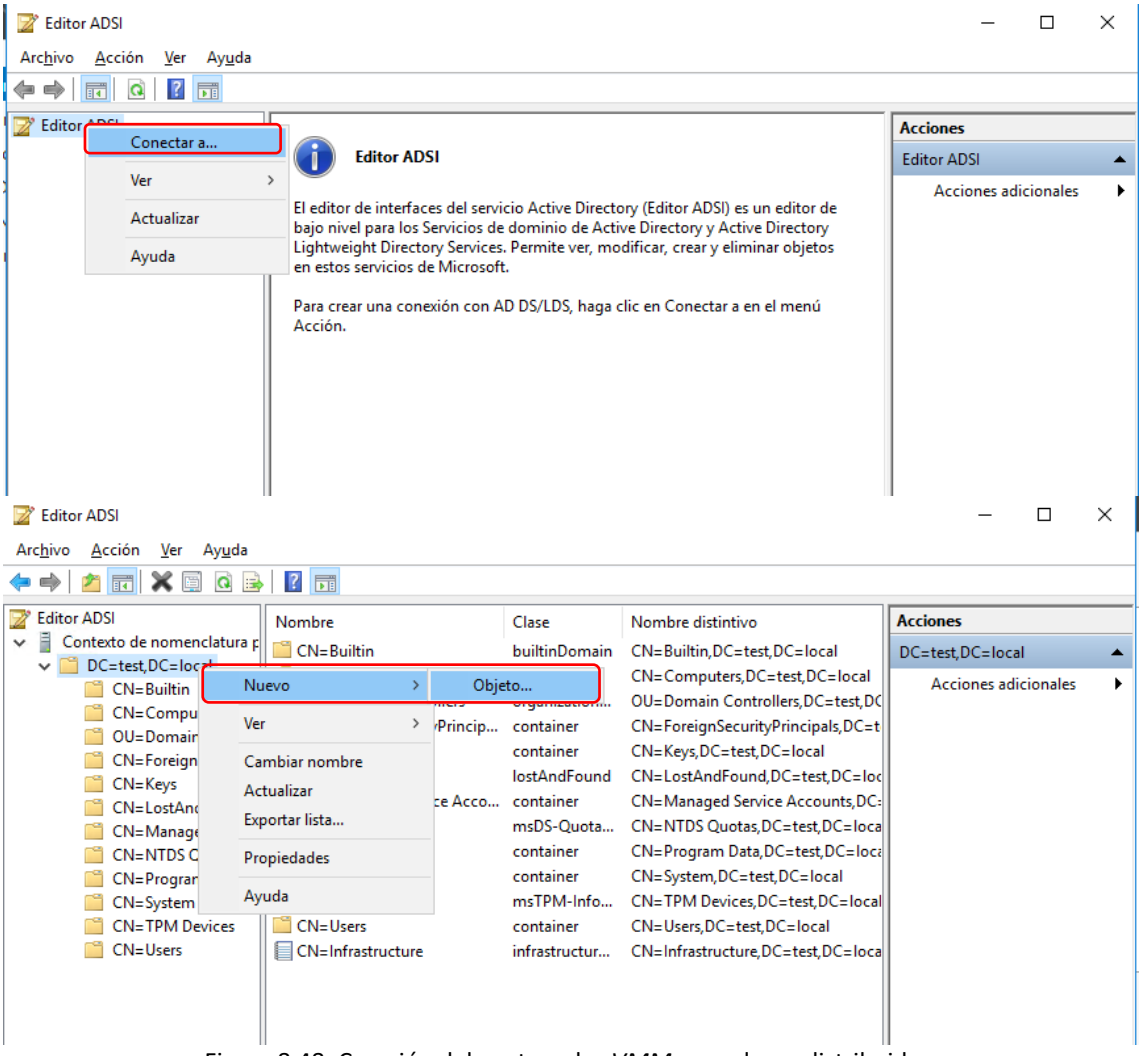


Figura 8.48: Creación del contenedor *VMM* para claves distribuidas.

Por último, debemos ofrecer control total al clúster sobre este nuevo contenedor. El proceso para hacerlo es el que sigue, y se muestra en la Figura 8.49.

i. Acceder a las propiedades del contenedor.
ii. Agregar el clúster: cluster-test.
iii. Ofrecer control total al clúster: cluster-test.
iv. Acceder a las opciones avanzadas.
v. Aplicar a los objetos cluster-test y al grupo de administradores: todos los descendientes.

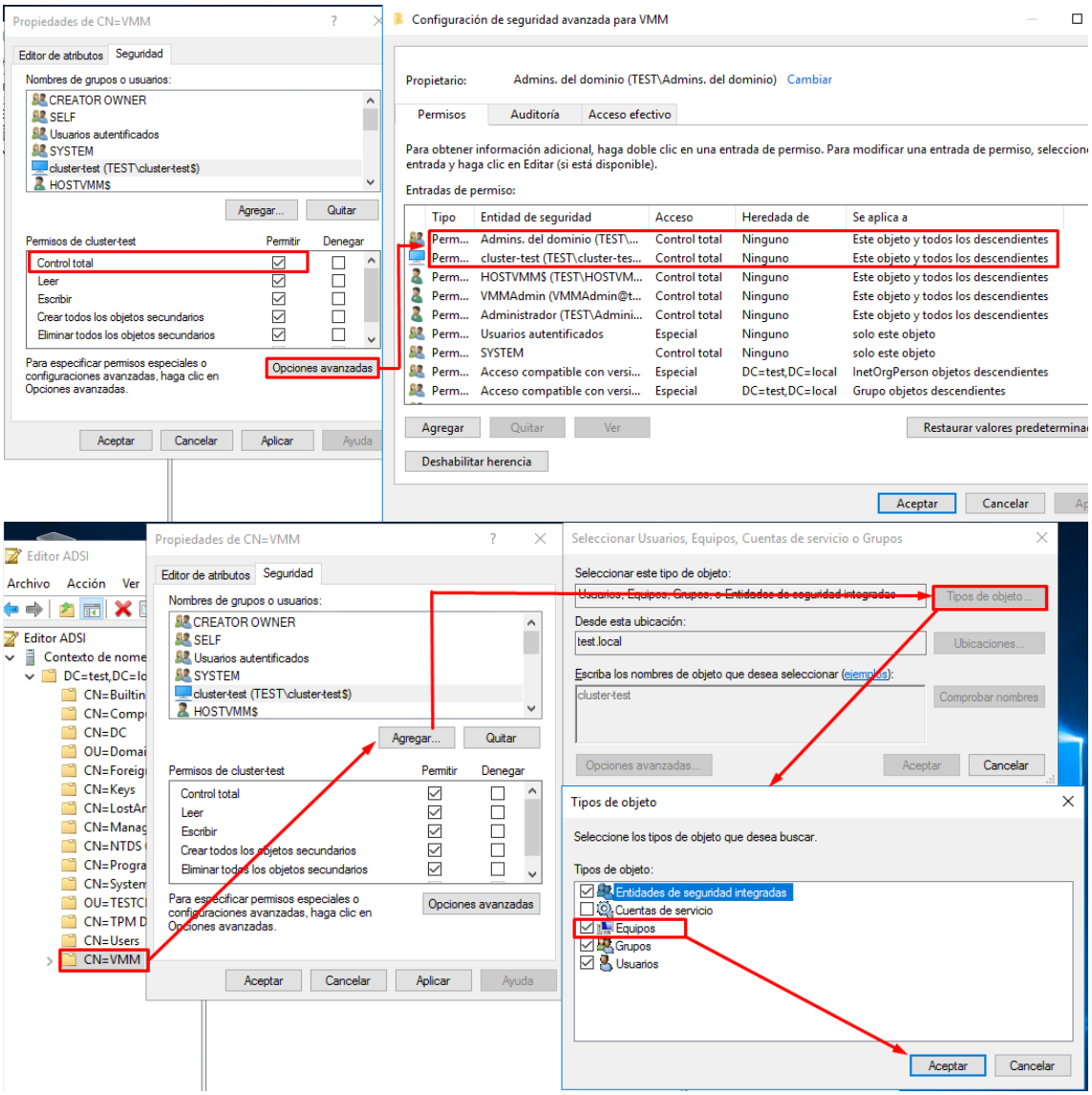


Figura 8.49: Permisos al clúster sobre el contenedor *VMM*.

Por último, antes de continuar con la instalación de *VMM*, hay que buscar la opción *distinguished name* para saber sus parámetros accediendo a las propiedades del contenedor, como muestra la Figura 8.50.

Así, ya podemos volver al asistente de instalación de *VMM* de la VM de servidor de *VMM* y seleccionar la opción *Almacenar mis claves en Active Directory*, utilizando la información del contenedor recientemente seleccionado, en nuestro caso: CN=VMM,DC=test,DC=local. El resto de las opciones se pueden dejar por defecto.

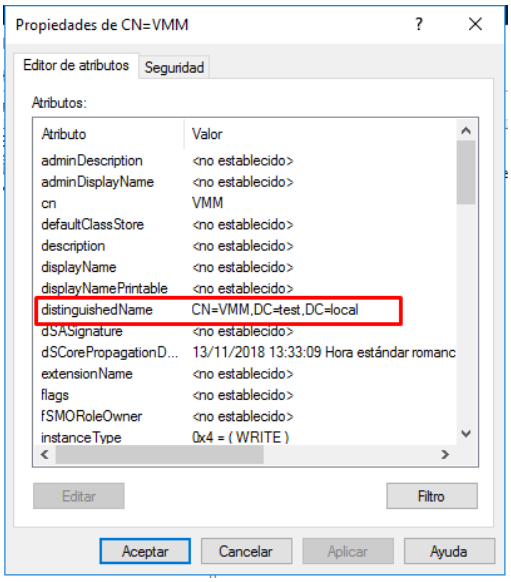


Figura 8.50: información del contenedor *VMM*.

8.3.2.3 Librería de VMM

Para configurar la librería remota de *VMM*, en nuestro caso se ha habilitado una ruta para compartir desde la propia VM: "C:\VMMLibrary Files". Esta carpeta se debe compartir con el clúster (cluster-test). En nuestro caso por facilidad se le ha ofrecido control total. Una vez hecho, el resto de configuración debe hacerse desde la consola de *VMM*.

8.3.2.4 Consola de VMM

Esta VM no se puede preparar hasta tener completamente instalado el sistema *VMM* en el servidor de *VMM*. Una vez instalado, se ejecuta de nuevo el asistente de instalación de *VMM*, pero seleccionando únicamente la opción de consola de *VMM*. Todas las opciones se pueden dejar por defecto.

Así, todas las VMs necesarias para el sistema están preparadas para poder iniciar *VMM*.

8.3.3 Configuración inicial de VMM previa a las pruebas

Una vez instalada, se puede ejecutar la consola para acceder al panel de *VMM* a través del nombre o IP del servidor de *VMM* con el puerto 8100 (por defecto) con que se nos haya asignado. Al ser el primer acceso, únicamente puede acceder el usuario del dominio *test**VMMAdmin*, como muestra la Figura 8.51. Llegados a este punto, y para finalizar esta fase, únicamente queda agregar la librería remota de *VMM* y el clúster de hosts para poder así gestionarlos.

Para agregar la librería remota, desde la sección *Tejido*, hay que hacer click derecho en *servidores de biblioteca*, y pulsar en *agregar un nuevo recurso de biblioteca*. Se abre entonces un asistente, donde se debe especificar una cuenta de ejecución. Esta cuenta no puede ser la misma que el usuario administrador de *VMM*. Por este motivo, se ha

creado un nuevo usuario miembro del grupo de administradores en el dominio. Lo siguiente que debemos indicar es el servidor de biblioteca, tal y como muestra la Figura 8.52.

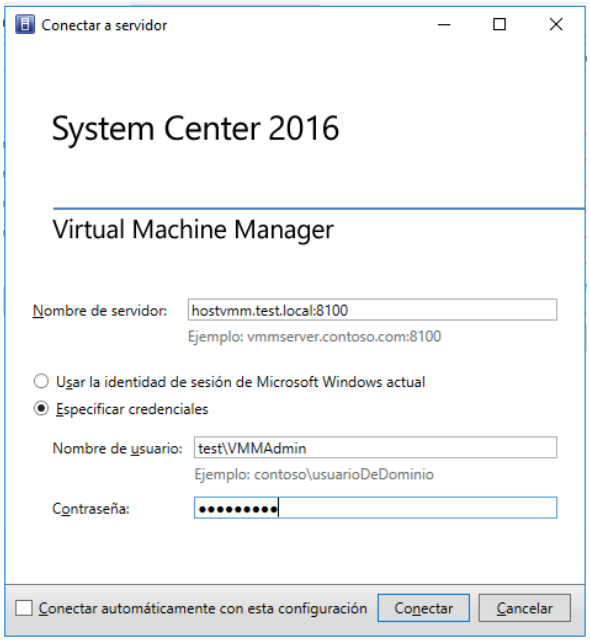


Figura 8.51: Consola de *VMM*.

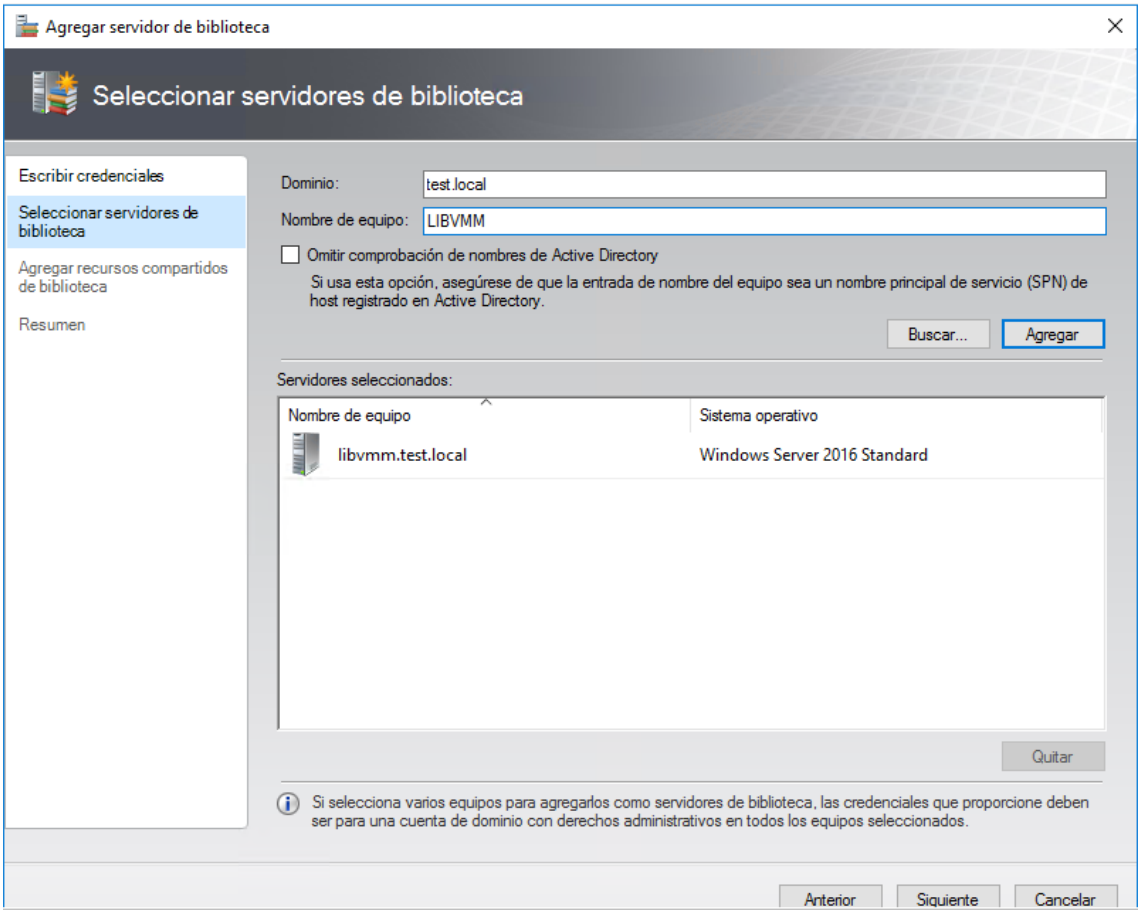


Figura 8.52: Agregar servidor de biblioteca.

Posteriormente se deben agregar los recursos compartidos de biblioteca. Si se ha hecho todo correctamente, debe aparecer la carpeta creada anteriormente para seleccionarla *VMMLibrary Files*. Una vez hecho, el servidor de biblioteca está listo para almacenar plantillas, principalmente.

Por último, queda agregar el clúster para poder gestionarlo. Previo a hacerlo, si se desea realizar la configuración de las redes sin que *VMM* haga configuraciones de manera automática, se debe desactivar la opción *crear redes lógicas automáticamente* en la sección de *Configuración*, como muestra la Figura 8.53.

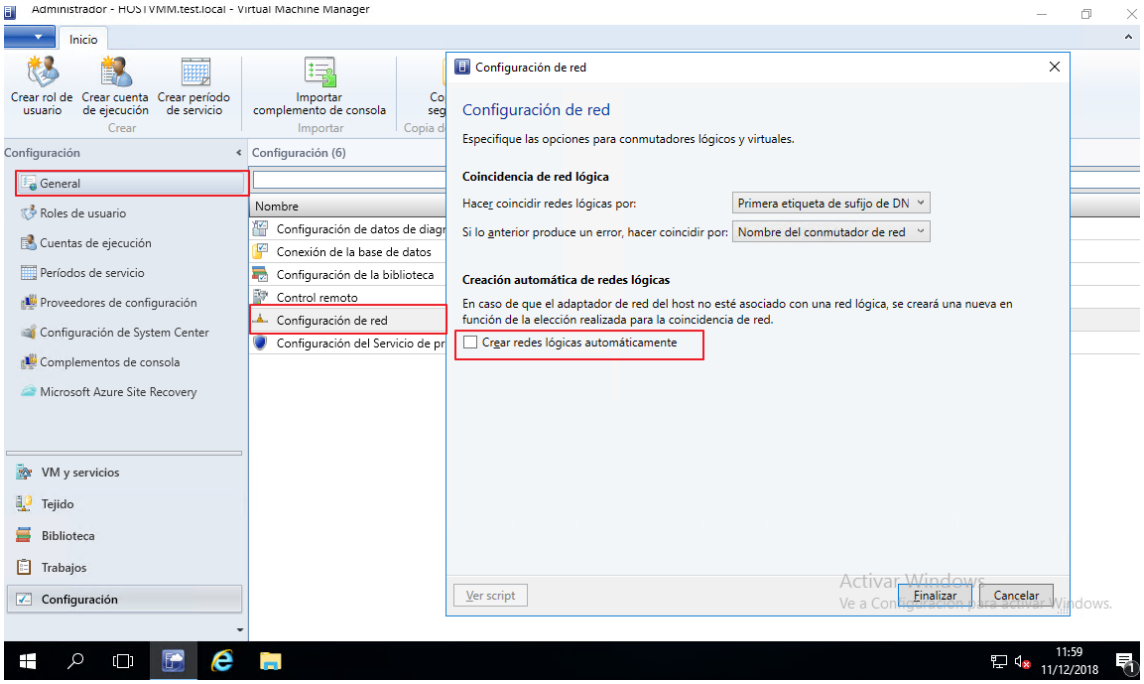


Figura 8.53: Deshabilitar la opción de creación de redes automáticamente.

Finalmente, para agregar el clúster, de nuevo en la sección *Tejido*, en el grupo *Todos los hosts*, se puede agregar directamente el clúster, o crear subcarpetas. Para obtener una mejor organización, se ha decidido en nuestro caso crear una subcarpeta para el clúster. Una vez creada, haciendo click derecho sobre esta nueva carpeta, se pulsa en la opción *Agregar hosts y clústeres de Hyper-V* para poder agregarlos, tal y como muestra la Figura 8.54.

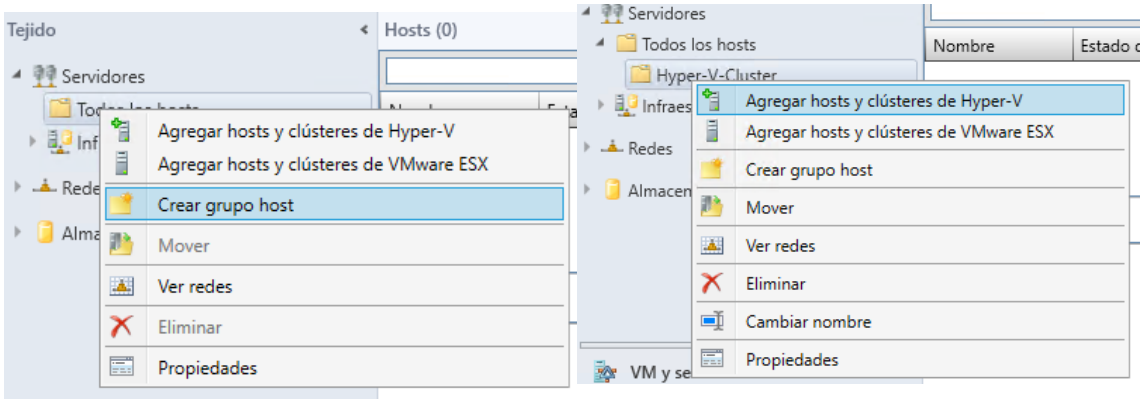


Figura 8.54: Agregar clúster a *VMM*.

Se abre un asistente para poder agregar el clúster. En la sección de *ubicación de recursos* se debe especificar *equipos de Windows server en un dominio de active directory de confianza*. En la sección de credenciales, se debe utilizar la cuenta de administrador creada anteriormente: test\administrador. En la siguiente ventana se pueden buscar los hosts o el clúster, especificando el nombre del clúster, o el nombre de los hosts de Hyper-V. En nuestro caso, se ha especificado los hosts, como muestra la Figura 8.55. Al pasar a la siguiente ventana, aparecen los hosts y su clúster, como muestra la Figura 8.56.

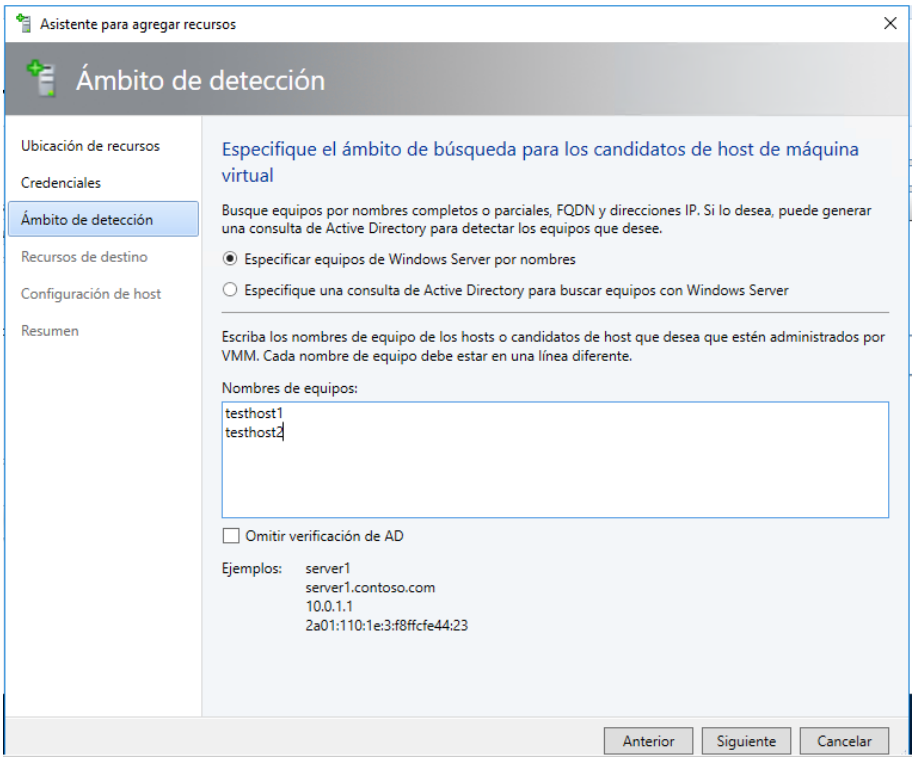


Figura 8.55: Agregar los hosts.

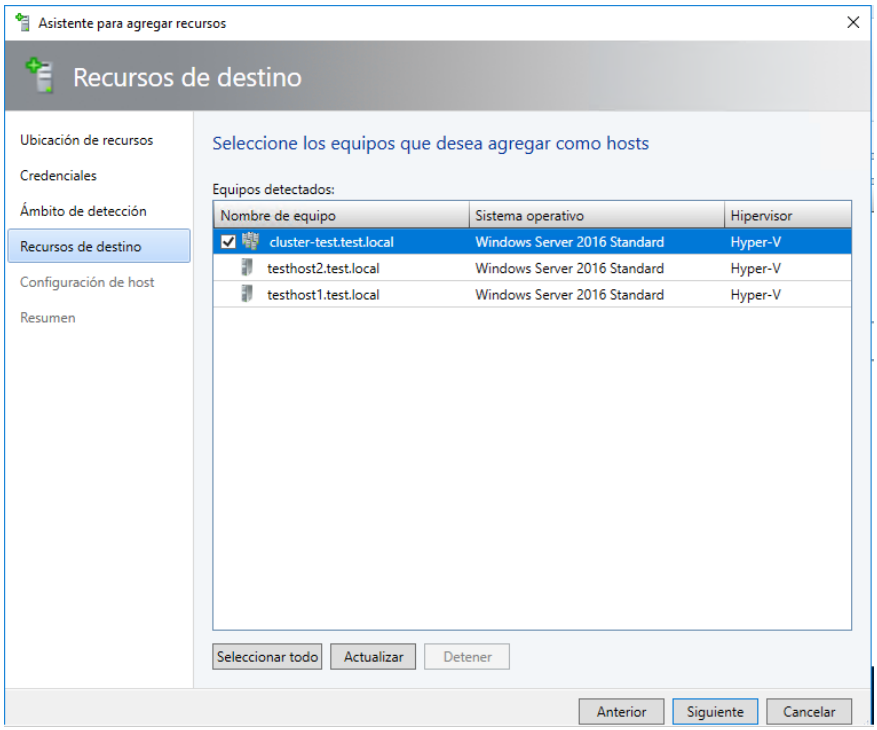


Figura 8.56: Agregar el clúster.

Para finalizar este proceso, se pueden dejar las opciones por defecto. De esta manera termina la preparación del entorno físico y así se pueden iniciar las pruebas de la herramienta *VMM*.

Desarrollo del proyecto: Pruebas del sistema *SCVMM*

En las siguientes secciones detallarán las características de *VMM* y las ventajas de su utilización frente a la gestión tradicional, es decir, sin *VMM*.

VMM se divide en tres partes o secciones a las que se puede acceder desde el menú principal ubicado en la esquina inferior izquierda, como muestra la Figura 9.1:

i. **Tejido**: En esta sección se puede configurar y ver el estado de la infraestructura de *VMM*, gestionar los hosts de virtualización y configurar las redes del entorno.
ii. **Biblioteca**: La biblioteca es un recurso compartido de archivos utilizados para implementar VMs y servicios en el tejido de *VMM*. Se almacenan recursos basados en archivos (discos duros virtuales, imágenes ISO…), recursos no basados en archivos (plantillas de VM y servicio) y VMs sin conexión almacenadas en la biblioteca.
iii. **VM y servicios**: En esta sección se pueden ver y gestionar las VMs y servicios, además de gestionar las redes de VM. Estas redes se asocian a redes lógicas y son las utilizadas para ofrecer conexión a las VMs. Se pueden implementar VMs y servicios ya sea creándolos desde cero, o mediante la utilización de plantillas.

Además, cuenta con un cuarto apartado, *Configuración*, donde se pueden realizar configuraciones propiamente de *VMM*. En este apartado es también donde se crean los perfiles de usuario, que se detallarán en la sección 9.4. Estas secciones se detallan a continuación.

Figura 9.1: Secciones de VMM.

9.1 Tejido

Como se ha mencionado anteriormente, en esta sección se gestiona la infraestructura que compone *VMM*. Esta infraestructura está compuesta por los servidores de *VMM* y bibliotecas, los clústeres de virtualización y las redes virtuales, entre las cuales están las *redes lógicas*, conectadas a los adaptadores de red físicos de los hosts de virtualización.

Una de las características de *VMM* es poder obtener información rápida sobre el tejido, accediendo al apartado de *Información general*, situado en el menú superior. Un ejemplo de la información que se obtiene se muestra en la Figura 9.2. Entre otras cosas, se observa un resumen de:

i. Cantidad de VMs existentes.
ii. Memoria RAM o almacenamiento disponible.
iii. Cantidad de VMs conectadas a cada red.
iv. Redes disponibles de cada host.

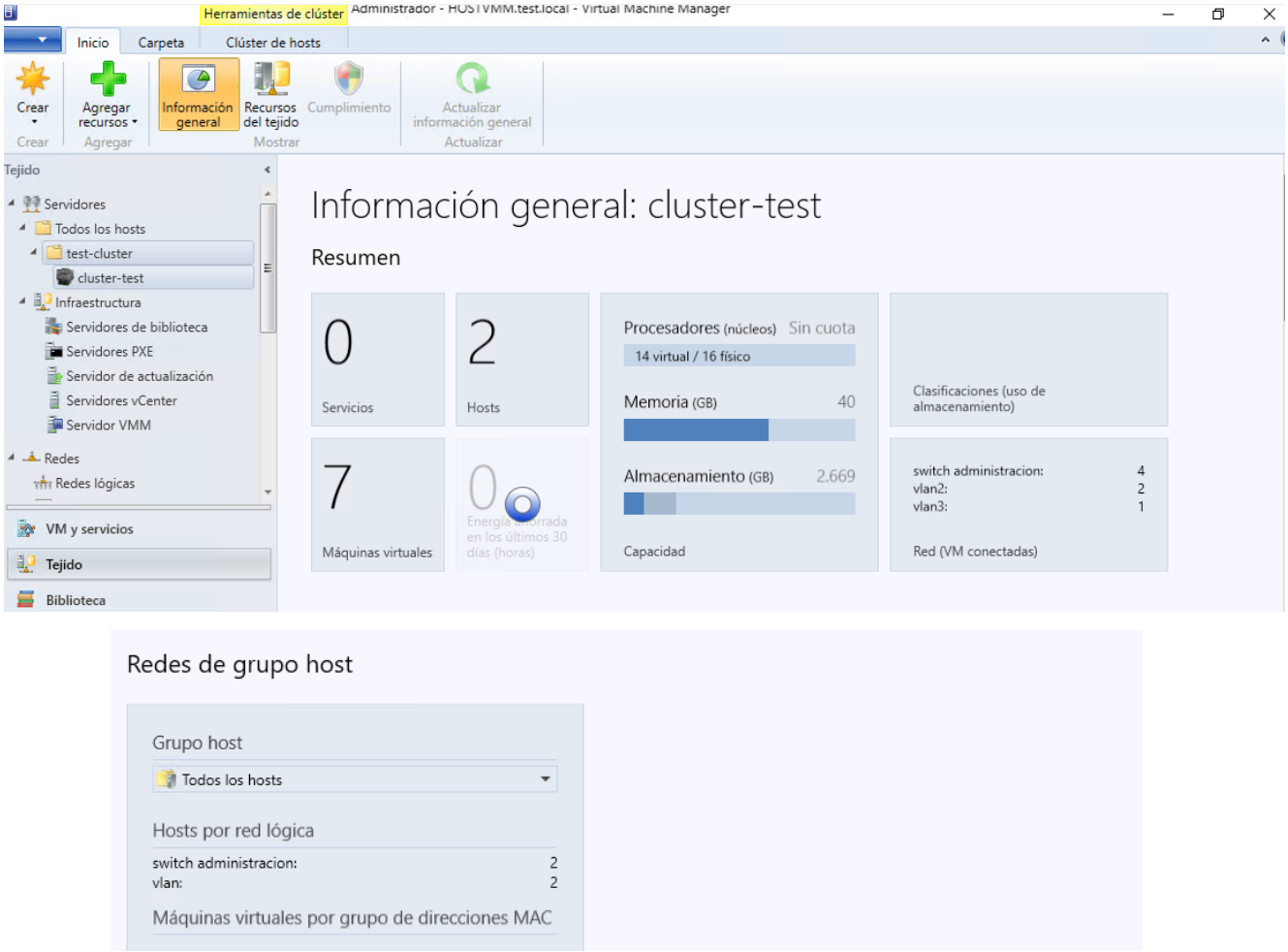


Figura 9.2: Información general de Tejido.

Poder observar las redes disponibles era uno de los puntos importantes mencionados en la sección 4. Es importante poder comprobar que se ha hecho correctamente la

configuración de red en todos los hosts. De esta manera se asegura que las VMs puedan migrar en caso necesario. Sin *VMM* esta configuración debe realizarse igual que se detalla en la sección 8.2.3, creando los teams de tarjetas de red y creando el conmutador virtual para cada host desde Hyper-V. En *VMM* es similar, sin embargo, permite comprobar que se ha hecho correctamente (con el mismo nombre de conmutador para todos los hosts), sin necesidad de tener acceso físico a los hosts.

Antes de demostrar el proceso en *VMM*, es necesario explicar las redes lógicas. Las redes lógicas deben ser una representación lo más fidedigna posible de la estructura de red física del datacenter. Así pues, estas redes son a las que se deben conectar las tarjetas de red de los hosts. Es importante indicar que si se han configurado conmutadores virtuales desde Hyper-V, *VMM* crea las redes lógicas correspondientes de manera automática. Esta opción la puede desactivar el administrador de *VMM* desde el apartado *Configuración,* como muestra la Figura 9.3.

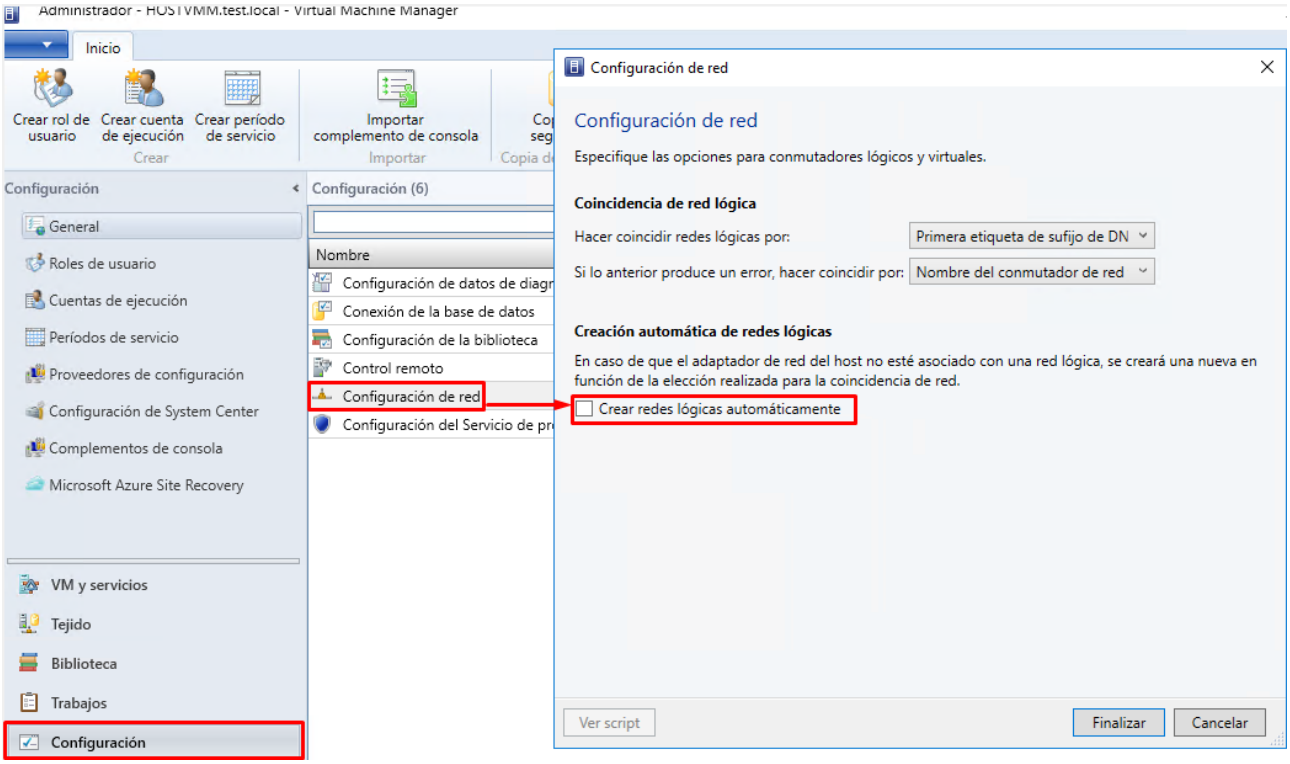


Figura 9.3: Opción de creación de redes lógicas automáticamente.

Desactivando esta opción se pueden configurar las redes tal y como se desee. En nuestro caso, realizando las pruebas una de las redes creadas automáticamente se ha eliminado para así poder probar otro tipo de red lógica basada en VLAN. Esta opción permitirá aumentar la seguridad en el *Cloud* de manera relativamente sencilla. Sin *VMM*, implementar una configuración de redes como la que se mostrará a continuación se hace de manera mucho más tediosa. Para crear nuevas redes lógicas, se debe escoger la opción pulsando click derecho sobre *Redes lógicas,* como muestra la Figura 9.4.

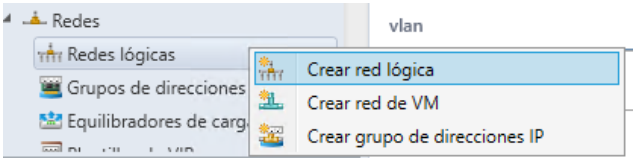


Figura 9.4: Creación de nueva red lógica.

Al hacerlo, se abre un asistente donde poder especificar un nombre. Seguidamente, se debe escoger el tipo de red que se desea crear. Los tipos de red se muestran en la Figura 9.5 y son:

i. **Una red conectada:** Este tipo de red no dispone de aislamiento físico, aunque se puede utilizar con aislamiento virtual para las VMs. Es la que se crea por defecto al agregar los hosts al *VMM* si no se deshabilita la opción de *creación de redes lógicas automáticamente*.

ii. **Redes independientes basadas en VLAN:** Este tipo de red es en la que nos hemos centrado para las pruebas debido a que permite dividir la red en sitios de red independientes, y así aislar cada grupo de VMs. Esto significa que cada VM puede ver únicamente las que pertenecen a su misma VLAN, a pesar de estar conectadas mediante la misma red física.

iii. **Redes VLAN privadas (PVLAN):** Este tipo de red se basa en sub-VLANs (o secundarias), es decir, en agrupaciones aisladas de VMs dentro de una VLAN primaria.

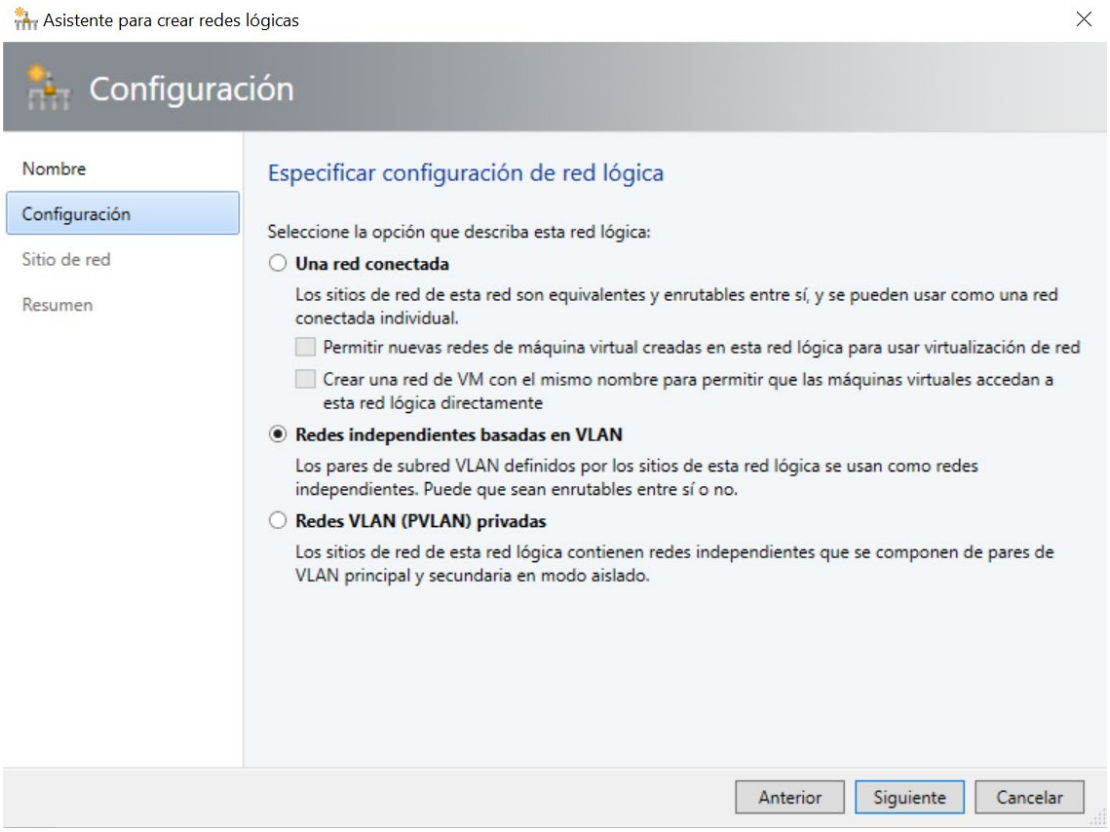


Figura 9.5: Tipos de red lógica.

Una vez escogido el tipo de red, en nuestro caso VLAN, se pueden agregar las subredes IP con su VLAN (red de área local virtual) asociada. En nuestro caso, por ejemplo, se han creado, entre otras, las que muestra la Figura 9.6.

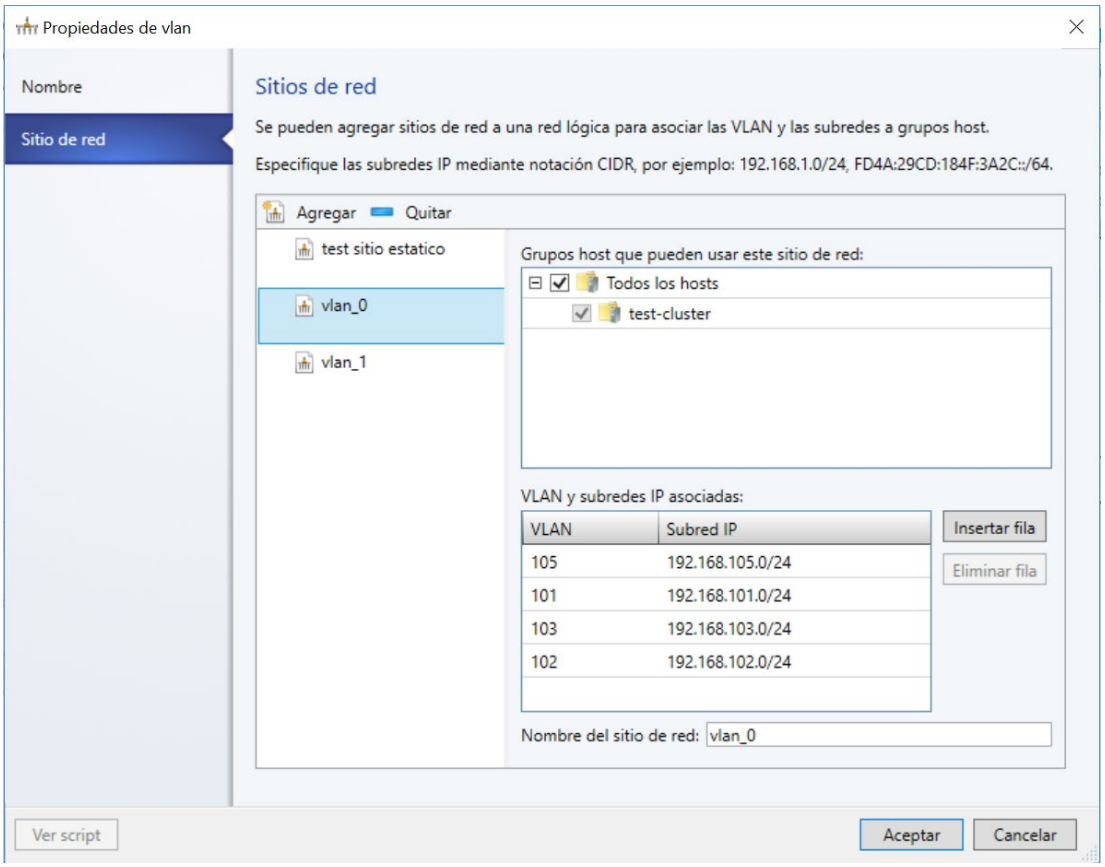


Figura 9.6: VLAN y su correspondiente IP en red lógica basada en VLAN.

Una vez se termine de crear las VLAN necesarias, hay que asociar las redes lógicas con los adaptadores de red físicos de los hosts. Se recomienda asociar todas las redes lógicas de un clustes a todos los hosts del cluster, ya que eso nos permitirá ejecutar cualquier VM del cluster en cualquier host. Para ello, deberemos acceder a las propiedades de hardware de cada host, y asociar el team creado anteriormente desde Hyper-V, con la red lógica, como se muestra en las figuras 9.7 y 9.8.

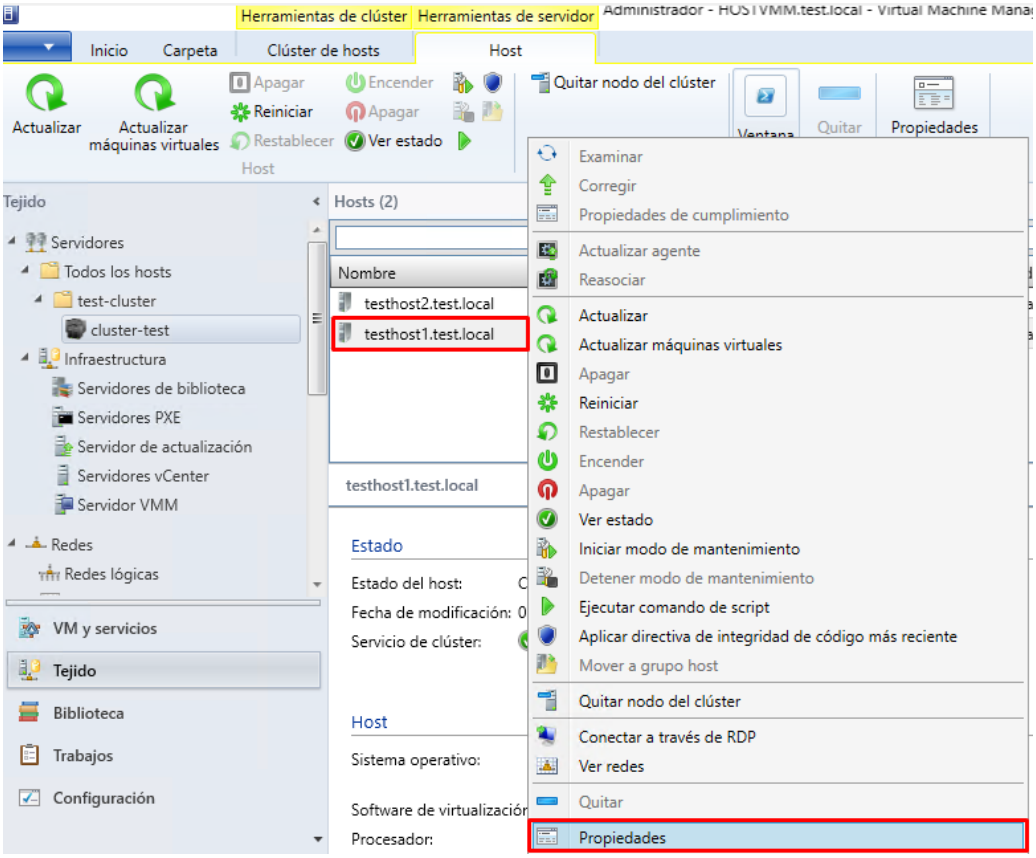


Figura 9.7: Acceso a las propiedades del host.

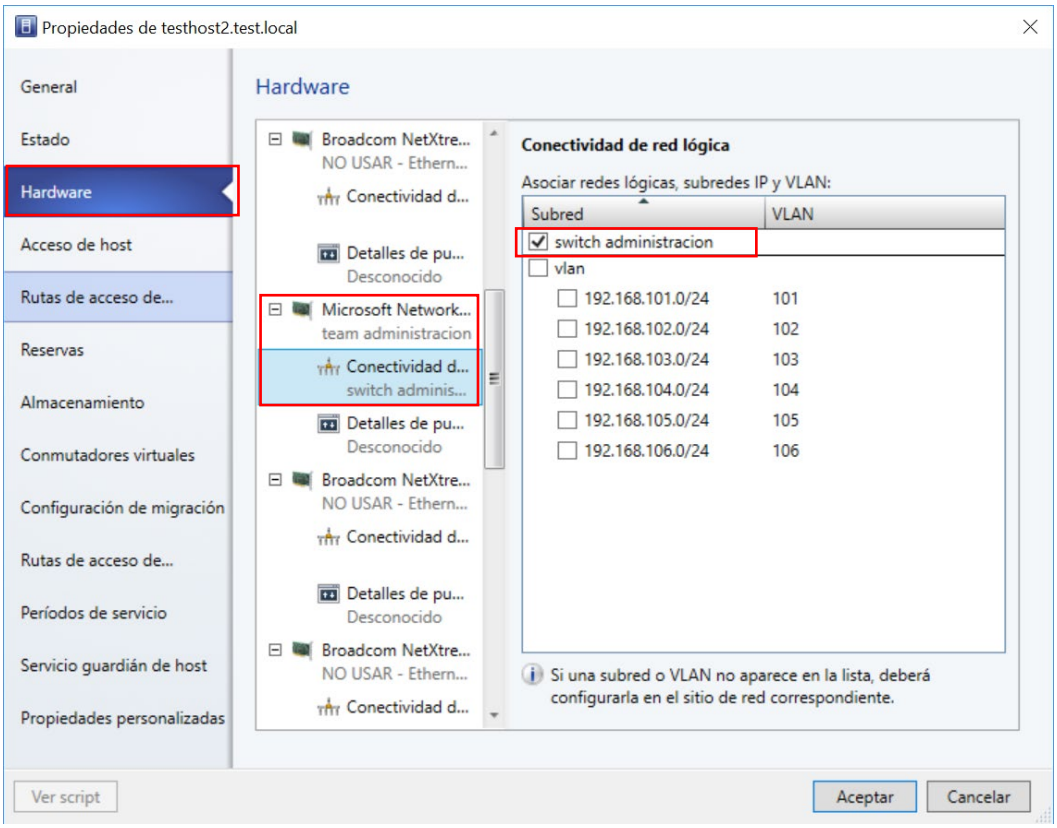


Figura 9.8: Conectividad de team con red lógica.

Una vez se han conectado todos los teams con su respectiva red lógica, se pueden configurar los conmutadores virtuales (estándar o lógicos)[1]. Este proceso se muestra en las Figuras 9.9 y 9.10.

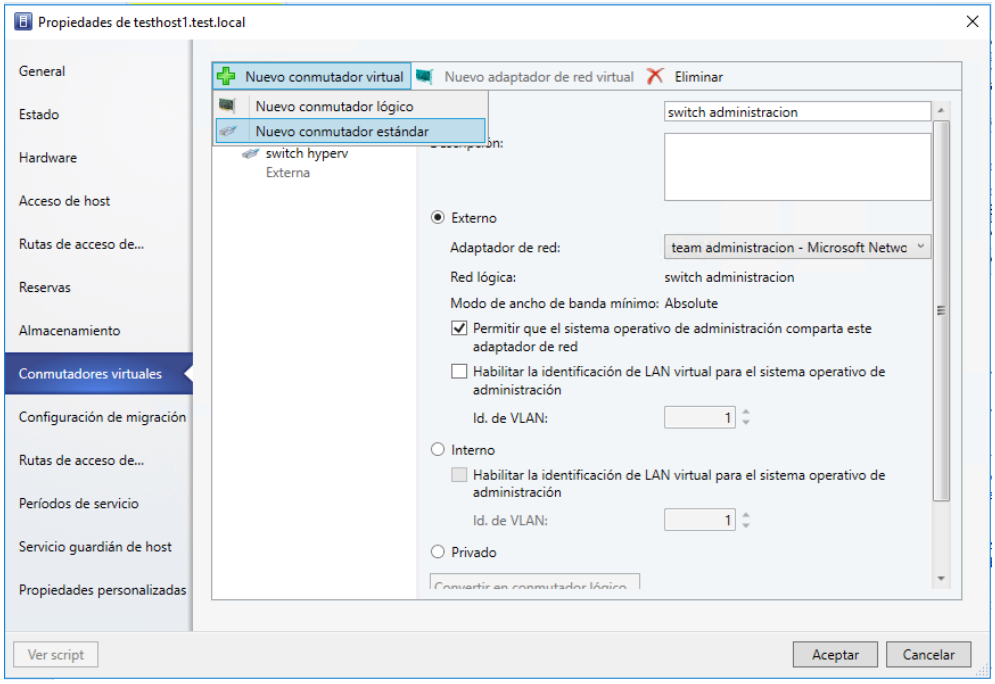


Figura 9.9: Creación de nuevo conmutador virtual.

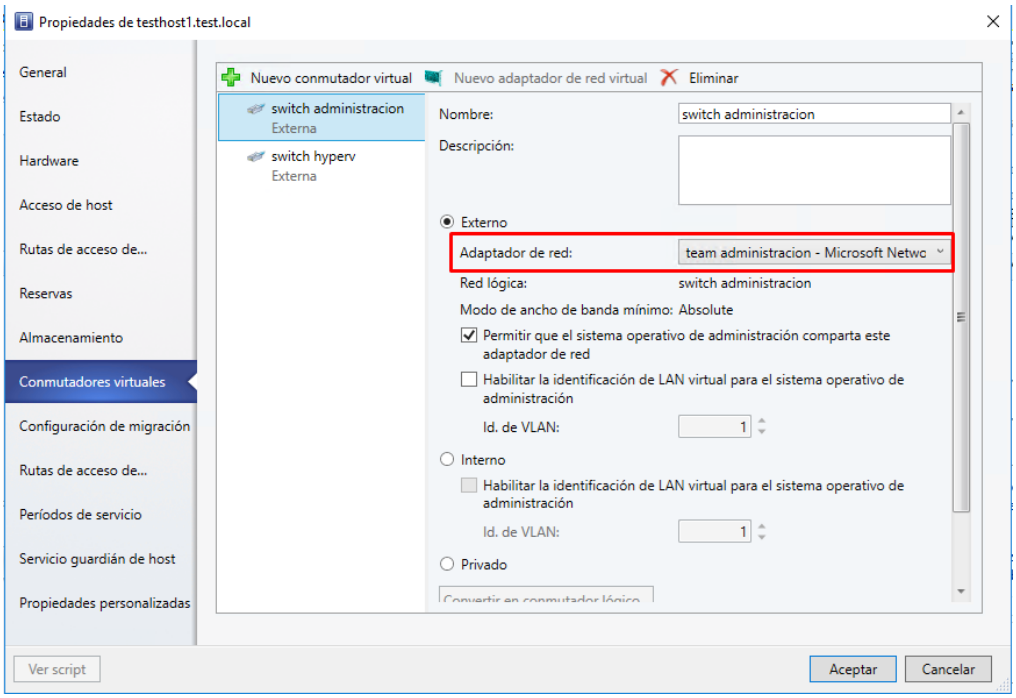


Figura 9.10: Conexión del conmutador virtual con el team creado anteriormente.

[1] Los conmutadores estándar son los nativos de Hyper-V, y son los encargados de enlazar los recursos de red virtuales (tarjetas de red de las VMs) con los físicos (tarjetas de red del host de virtualización. Los conmutadores lógicos se utilizan para aplicar configuraciones específicas básicamente a través de los perfiles de puerto (gestión de ancho de banda, seguridad de red capa 2, acceso directo a recursos…).

Si previamente se han configurado conmutadores virtuales desde Hyper-V, ya aparecerán esos conmutadores. En ese caso, sencillamente habría que comprobar que el nombre se corresponda con el de los demás hosts, y conectar el conmutador al adaptador de red correspondiente. En la Figura 9.10 se muestra como el conmutador virtual "switch administración" está conectado al adaptador de red "team administración", que a su vez está conectado a la red lógica "switch administración". Esta red se creó automáticamente al añadir el host a *VMM*, por ese motivo tiene el mismo nombre que el conmutador, convendría modificar el nombre de esta para no confundirla con el conmutador virtual.

Este proceso debe hacerse para todos los hosts, por lo tanto, la cantidad de trabajo a realizar es el mismo que sin utilizar *VMM*. Sin embargo, una vez terminado, utilizando *VMM* se pueden ver las redes del clúster como muestra la Figura 9.11 para comprobar que se haya hecho correctamente y evitar futuros problemas.

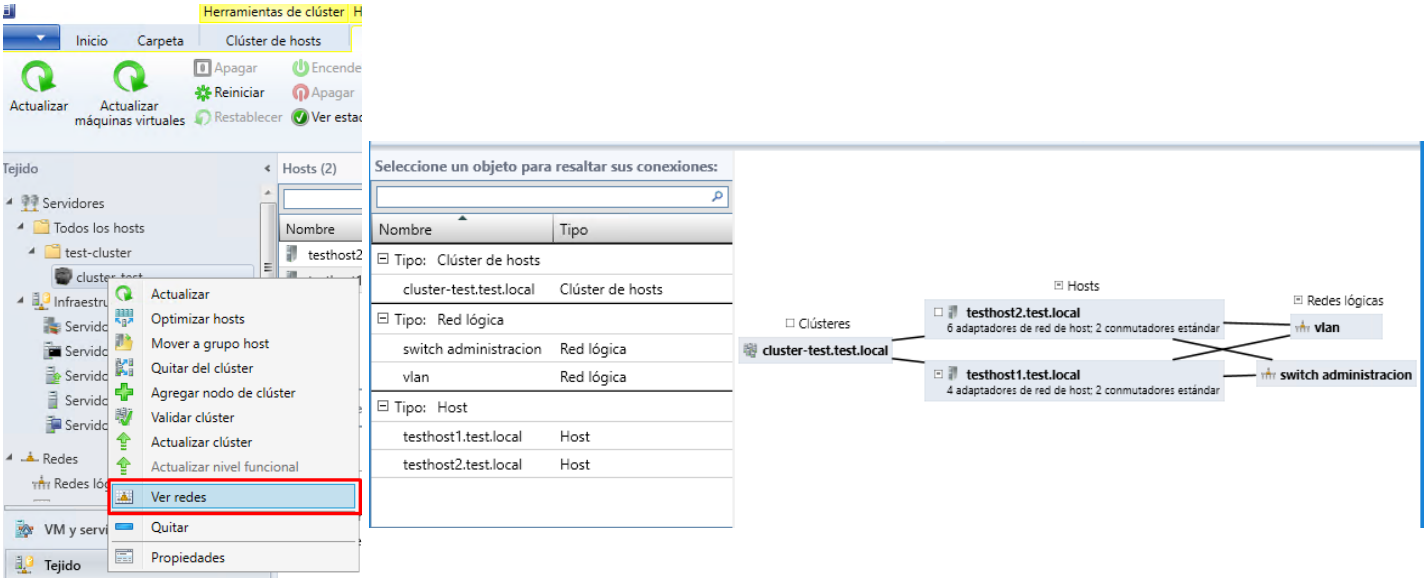


Figura 9.11: Comprobación de las redes de clúster.

Nota

Se pueden crear grupos de direcciones mac y grupos de direcciones IP que se encargarán de asignar automáticamente estas direcciones a las redes virtuales. Los grupos de direcciones IP se deben asociar tanto a redes lógicas como redes de VM, y los de direcciones mac a los propios hosts de virtualización.

9.2 Biblioteca

La principal característica de la biblioteca es la creación de plantillas. Estas se clasifican de la siguiente manera:

i. Plantillas de VM.
ii. Plantillas de perfiles.
iii. Plantillas de servicio.

9.2.1 Plantillas de VM

Estas plantillas se crean como muestra en la Figura 9.12. Existen varias opciones de creación:

i. Utilizar otra plantilla de VM o un disco duro virtual ya almacenado en biblioteca.
ii. Utilizar una VM existente en un host.

Las personalizaciones de la plantilla disponibles al escoger la primera opción son principalmente la modificación de opciones de configuración de hardware o sistema operativo. Escoger la segunda opción permite personalizar las opciones sistema operativo. Sin embargo, las de hardware no se pueden modificar en el momento de crear la plantilla. Entre las opciones de sistema operativo, se pueden seleccionar las características y roles de Windows Server que sean necesarias. Esta opción elimina la VM existente. Para ambos casos se pide seleccionar la ubicación de biblioteca en la que se desea almacenar la plantilla, como muestra la Figura 9.13.

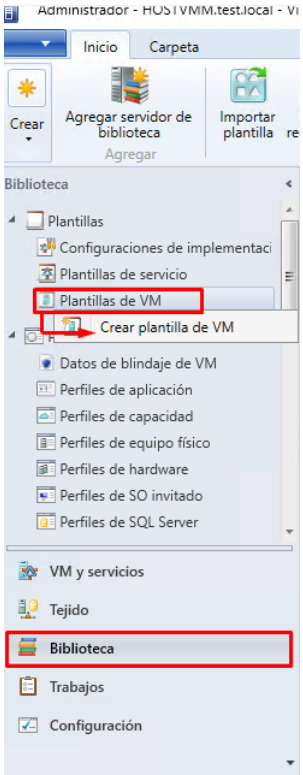


Figura 9.12: Creación de nueva plantilla.

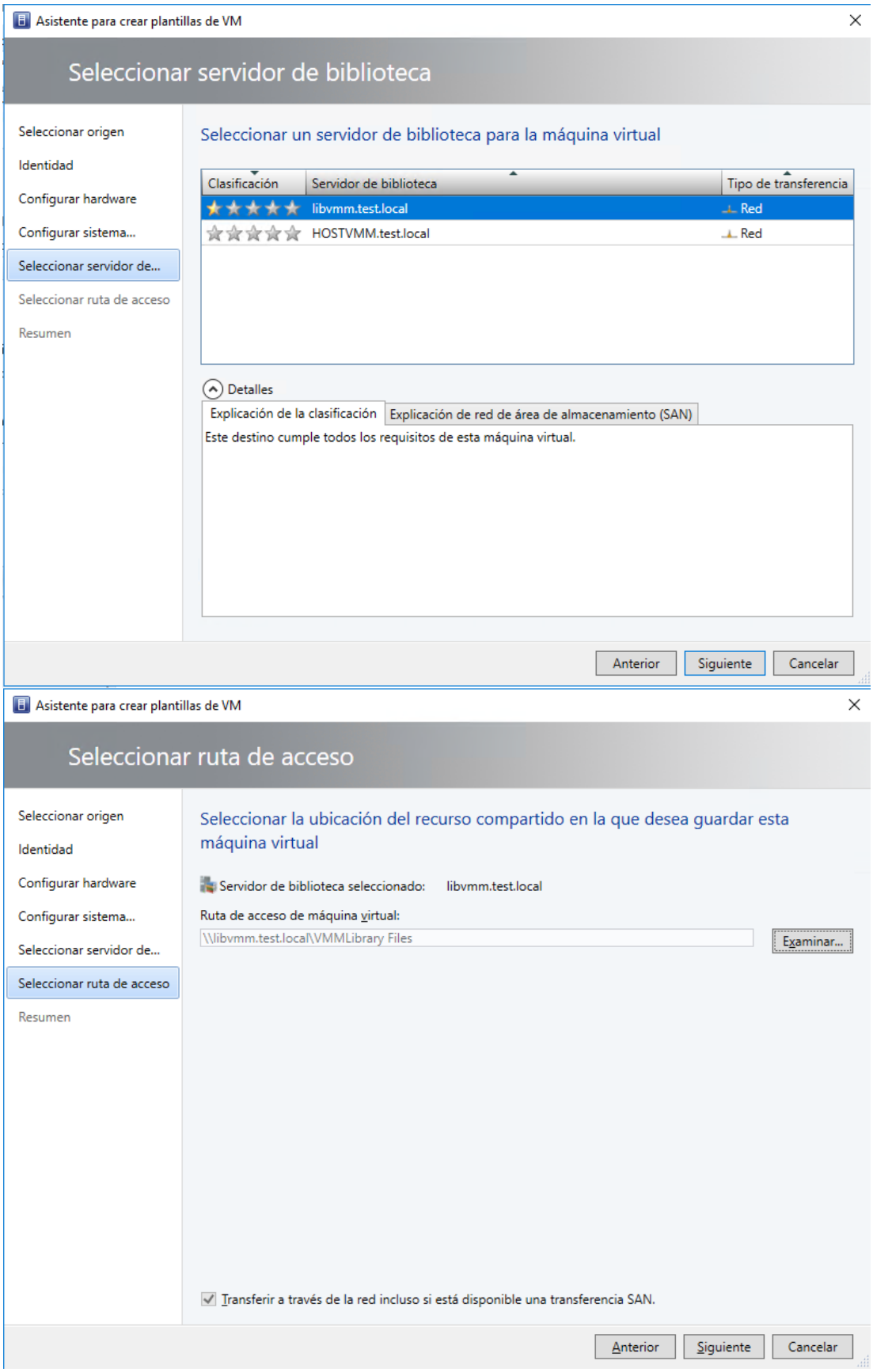


Figura 9.13: Selección de biblioteca y recurso compartido.

Una vez finalizado el asistente, se puede ver el proceso del trabajo en la sección *Trabajos* como muestra la Figura 9.14. En esta sección, se puede visualizar el trabajo actual, además de un histórico de trabajos y detalles de cada uno.

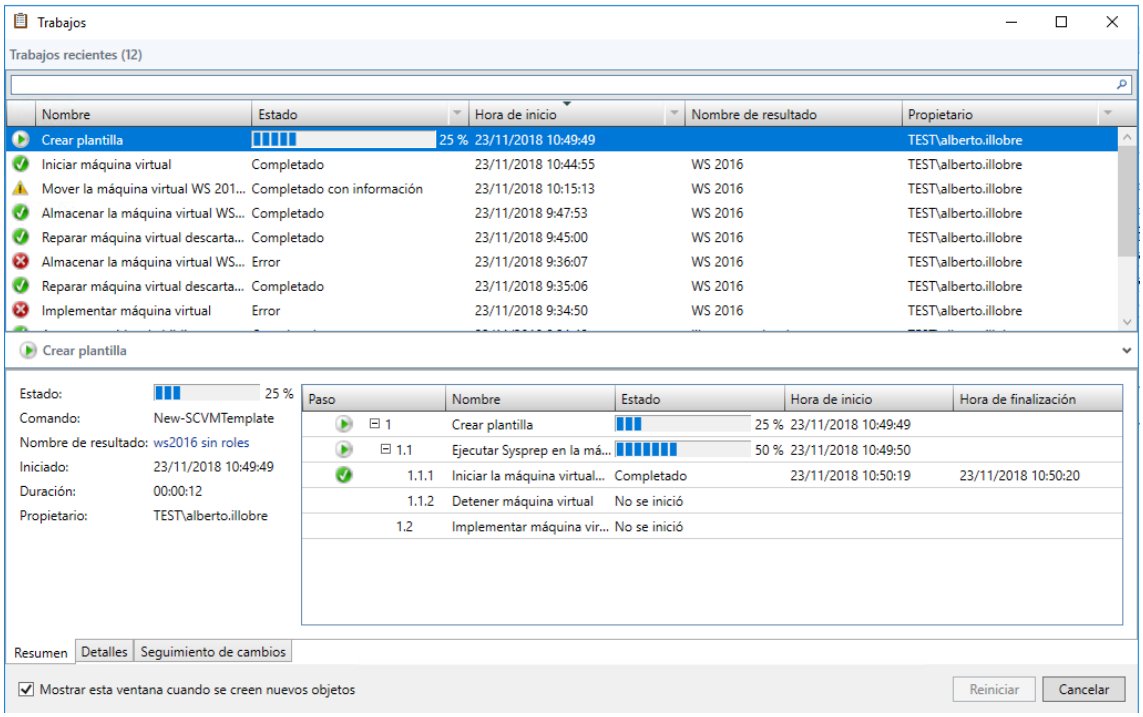


Figura 9.14: Sección Trabajos.

9.2.2 Plantillas de perfiles

En este apartado se pueden crear perfiles de varios tipos para utilizar en las plantillas de VM, plantillas de servicio o al crear VMs. Los perfiles que se pueden crear y sus detalles se muestran en la Tabla 9.1.

Perfil	Detalles	Usado en plantillas de VM	Usado en plantillas de servicio
Perfil de hardware	Define la configuración de hardware, como la CPU, memoria, adaptadores de red, un adaptador de video, una unidad de DVD y la prioridad de VM cuando los recursos se asignan en un host de VM.	Sí	No
Perfil de sistema operativo invitado	Define opciones de configuración del sistema operativo que se aplican a una VM, incluido el tipo de sistema de VM, el nombre de equipo, contraseña de administrador, nombre de dominio, clave de producto, zona horaria, archivo de respuesta y archivo RunOnce.	Sí	No
Perfil de aplicación	Proporciona instrucciones para instalar una aplicación. *VMM* admite varios mecanismos para la implementación de aplicaciones.	No	Sí

Perfil de SQL Server	Proporciona instrucciones para personalizar una instancia de Microsoft SQL Server para un DAC de SQL Server cuando se implementa una máquina virtual como parte de un servicio.	No	Sí
Perfil de capacidad	Define límites y funcionalidades para un conjunto de recursos específico, por ejemplo, la configuración de adaptadores de red, intervalos de procesador y memoria. Los perfiles de capacidad se usan en perfiles de hardware o en implementaciones en la nube. Por ejemplo, puede configurar una nube privada y asignarla un perfil de capacidad de Hyper-V que requiera que todos los recursos tengan una disponibilidad alta. En este ejemplo debe configurar recursos de biblioteca, como perfiles de hardware, para que estén en línea con la capacidad.	Sí	Sí
Perfil de equipo físico	Define la configuración que se usa para aprovisionar servidores.	No	No

Tabla 9.1: Perfiles de *VMM*.

Teniendo en cuenta la sencillez de los perfiles, no hemos considerado necesario describir el funcionamiento mediante ejemplos. Cabe aclarar que estos perfiles pueden ser útiles en entornos muy dinámicos (donde se modifiquen las plantillas con asiduidad) pero no tanto en entornos más estáticos (como es en la mayoría de los casos).

Sin embargo, se ha creado un perfil de sistema operativo invitado para poder guardar una clave de producto y así poder desplegar VMs desde plantilla que, tal y como se detallará en la sección 9.3.7, requiere de licencia para evitar un error durante la creación de VM. De esta manera, se agilizan el resto de las pruebas.

9.2.3 Plantillas de servicio

A través de los servicios se puede implementar de forma desatendida una infraestructura de una o varias VMs con servicios asociados a cada una de ellas (p.ej. servidor Active Directory, servidor DNS, ejecución de scripts, etc.).

Las plantillas de servicio permiten configurar una o varias VMs para proporcionar una aplicación. Contienen información sobre un servicio, incluidas las máquinas virtuales que se implementan como parte del servicio, las aplicaciones instaladas en máquinas virtuales y la configuración de red que debe usarse. Se pueden agregar plantillas de máquina virtual, configuración de red, aplicaciones y almacenamiento a una plantilla de servicio. Las VM de las plantillas de servicio se pueden agregar según una copia de una plantilla de VM existente (que se puede personalizar) o un disco duro virtual en la biblioteca. Para crearlas, se puede hacer click derecho en *Plantillas de servicio*, o pulsar el icono que aparece en la parte superior izquierda, tal y como muestra la Figura 9.15.

Al hacerlo, se abre un asistente donde se puede crear un servicio utilizando uno, dos o tres niveles de VMs, o en blanco, como se puede observar en la Figura 9.16.

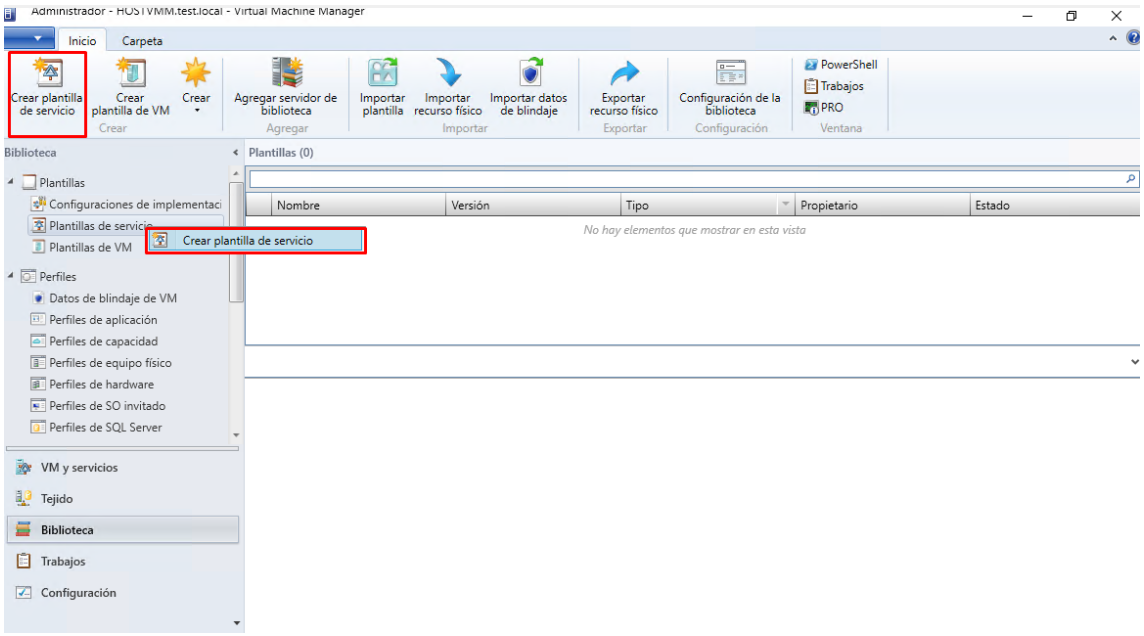


Figura 9.15: Creación de plantilla de servicio

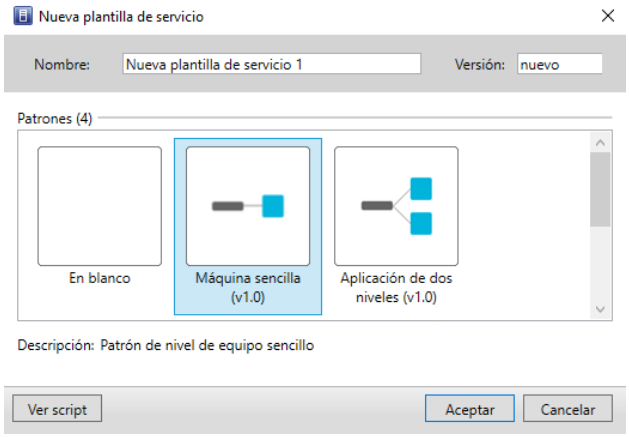


Figura 9.16: Niveles de plantilla de servicio.

Al escoger alguna de las opciones con una o varias máquinas, se abre el diseñador de la plantilla de servicio, donde aparecen a la izquierda las plantillas de VM de las que se dispone, y a la derecha se pueden modificar los valores de las VMs que se están configurando.

En la Figura 9.17 se muestra el diseño de una plantilla de servicio de *máquina sencilla* utilizando una plantilla de VM. Para agregar esta plantilla, simplemente debe arrastrarse hacia el diseñador. Una vez hecho, se pueden configurar el hardware y el S.O de la VM principalmente, haciendo doble click sobre la plantilla en el diseñador. Para esta configuración de S.O, se han realizado pruebas de instalación automática de roles y características de Windows Server.

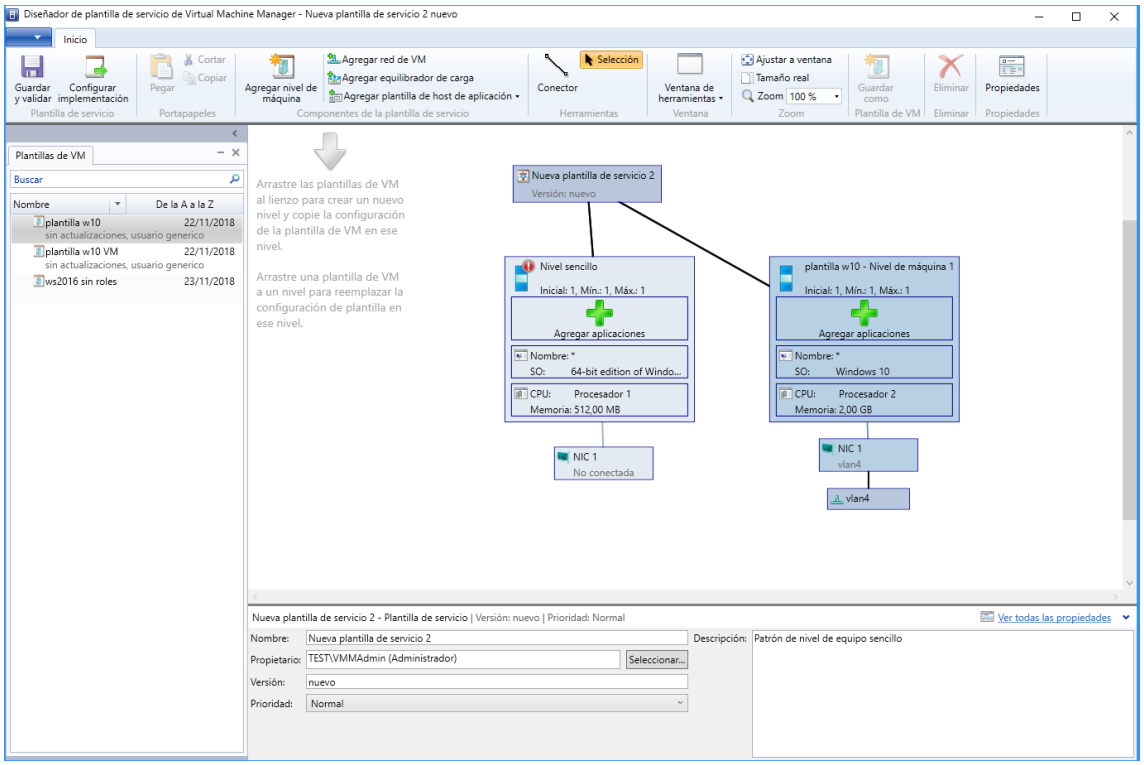


Figura 9.17: diseñador de plantilla de servicio.

Nota

Si se ha escogido crear la plantilla de servicio desde *máquina sencilla, dos niveles* o *tres niveles*, debe haber exactamente ese número de VMs en la plantilla, o provocará un error al intentar crear la plantilla de servicio.

9.2.4 Recursos de biblioteca

Por último, en la biblioteca se pueden consultar todos los recursos de que se dispone, además de poder añadir nuevos. Esto se puede hacer en el apartado *Servidores de biblioteca*, o seleccionando el servidor que interese observar, como muestra la Figura 9.18.

Para añadir nuevos recursos se puede hacer o bien añadiéndolos al recurso compartido de biblioteca del servidor correspondiente de manera manual, o utilizando la opción *importar recurso físico* ubicada en el menú de la parte superior. Una vez hecho, se debe agregar el recurso ubicado en el equipo local que se desee importar a *VMM* y seleccionar el servidor de biblioteca de destino al cual importar ese recurso. La Figura 9.19 muestra la interfaz para realizar estas acciones.

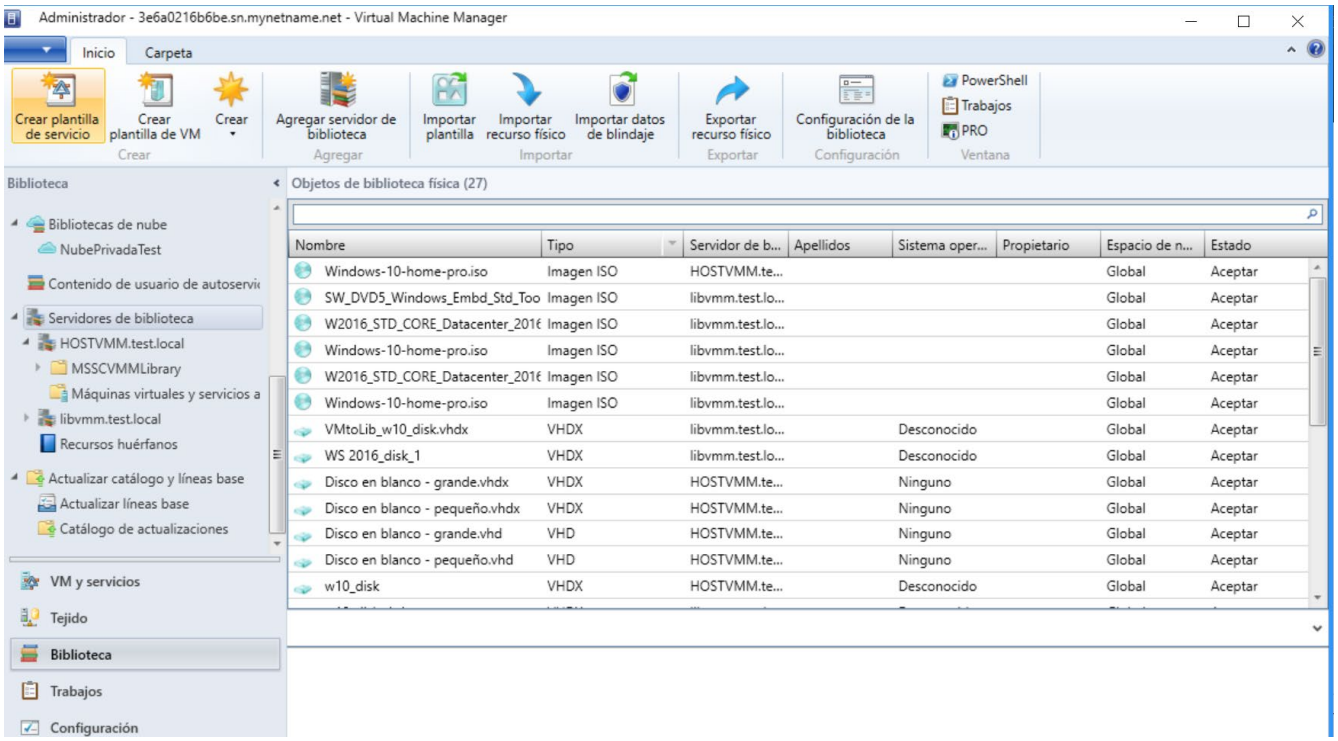


Figura 9.18: recursos de biblioteca.

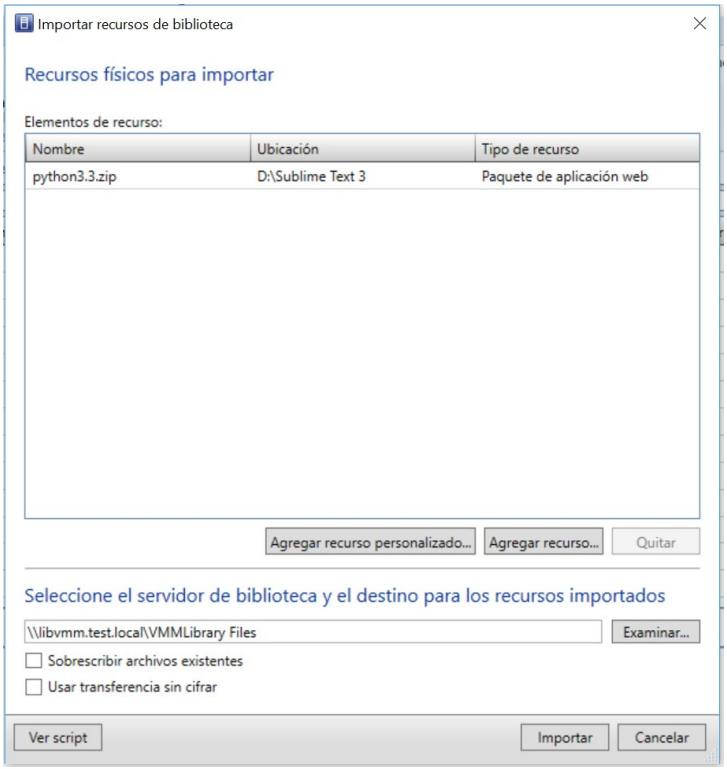


Figura 9.19: Importar recurso al servidor de biblioteca.

Al tener acceso al recurso compartido, en nuestro caso se ha decidido hacerlo siempre de manera manual. Los recursos que se pueden importar son los que admite la biblioteca, detallados en la sección 1.3.

9.3 VM y servicios

En esta sección se pueden observar y gestionar las VMs y servicios a los que el usuario conectado tenga acceso. Además, con los permisos adecuados, se puede ver a que host o *nube privada* pertenece cada VM. En esta sección también se pueden gestionar las redes de VM, las subscripciones de Azure y el almacenamiento de las VMs.

9.3.1 Nubes privadas

Las nubes privadas son la primera opción que aparece en el menú de VM y servicios, sin contar el apartado *Inquilinos*, que, aunque permite hacer click derecho para crear roles de usuario, no es en este apartado donde se gestionan específicamente. Por tanto, se explicarán en la sección 9.4. Las *nubes privadas* se pueden entender como un subconjunto de VMs para facilitar su gestión en entornos *Cloud* grandes. La Figura 9.20 muestra las dos opciones existentes para la creación de nubes privadas.

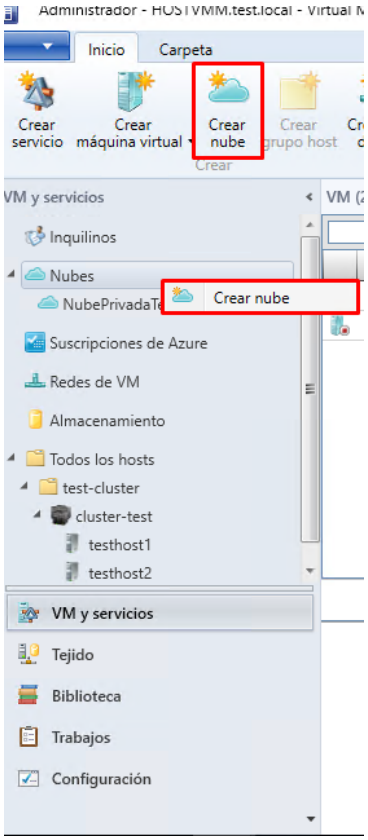


Figura 9.20: Nubes privadas.

Una vez seleccionada una de las dos opciones, se abre un asistente para poder crearlas. En este, entre otras cosas, se pueden definir:

i. Nombre y descripción.
ii. Recursos físicos a los que la nube privada tiene acceso (hosts o clústeres).
iii. Recursos de redes lógicas.

iv. Almacenamiento disponible.
v. Recursos de biblioteca para lectura.
vi. Capacidad de la nube: límite de CPUs virtuales, memoria, almacenamiento, VMs.
vii. Perfiles de capacidad.

La configuración de la nube se puede modificar posteriormente a su creación. Además, se pueden asignar usuarios a esas nubes, para que las VMs y servicios creados en esa nube los puedan gestionar dichos usuarios. A pesar de que exista la opción de crear VM y servicios en la nube privada, al hacer click derecho sobre la nube, aparece el mismo asistente que si se hiciese sin ser desde esta, por lo que se explicará en las secciones 9.3.6 y 9.3.6.

Estas nubes privadas permiten ofrecer a una organización una serie de recursos físicos para organizar su propio entorno *Cloud* sin necesidad de tener conocimiento sobre los recursos físicos subyacentes. De esta manera, los propietarios de estas *nubes privadas* podrían aumentar los recursos virtuales de sus VMs dentro de los límites de capacidad de su nube.

9.3.2 Integración con Azure

Microsoft permite integrar *VMM* con Azure Site Recovery[1] para así obtener seguridad en caso de caída del sistema. En *VMM* se pueden agregar suscripciones de Azure al servidor de *VMM* para que el *Cloud* pueda seguir funcionando en Azure hasta que se restablezca el sistema. Esta característica se implementará en otro proyecto, ya que permitiría ofrecer a los clientes una disponibilidad mucho mayor.

9.3.3 Redes de VM

Las redes de VM son las que se utilizan para dar conectividad a las VMs. Éstas se conectan a redes lógicas al crearlas. Por tanto, para poder crear redes de VM, primero es necesario crear redes lógicas. Una vez haya una red lógica disponible, se puede crear la red de VM como muestra la Figura 9.21. Al hacerlo, se abre un asistente, donde se debe escoger un nombre y una red lógica, y especificar las opciones de aislamiento. La red lógica engloba todas las VLANs que se hayan creado en esta. En las opciones de aislamiento, como se muestra en la Figura 9.21, se puede escoger una VLAN específica. Si la red lógica no es VLAN, no aparece la opción *Opciones de aislamiento*.

[1] Azure es la nube de Microsoft que permite compilar, implementar y administrar rápidamente aplicaciones en una red glocal de datacenters. Azure Site Recovery permite asegurar la continuidad del servicio *Cloud* durante las interrupciones, manteniendo las aplicaciones y cargas de trabajo empresariales en funcionamiento.

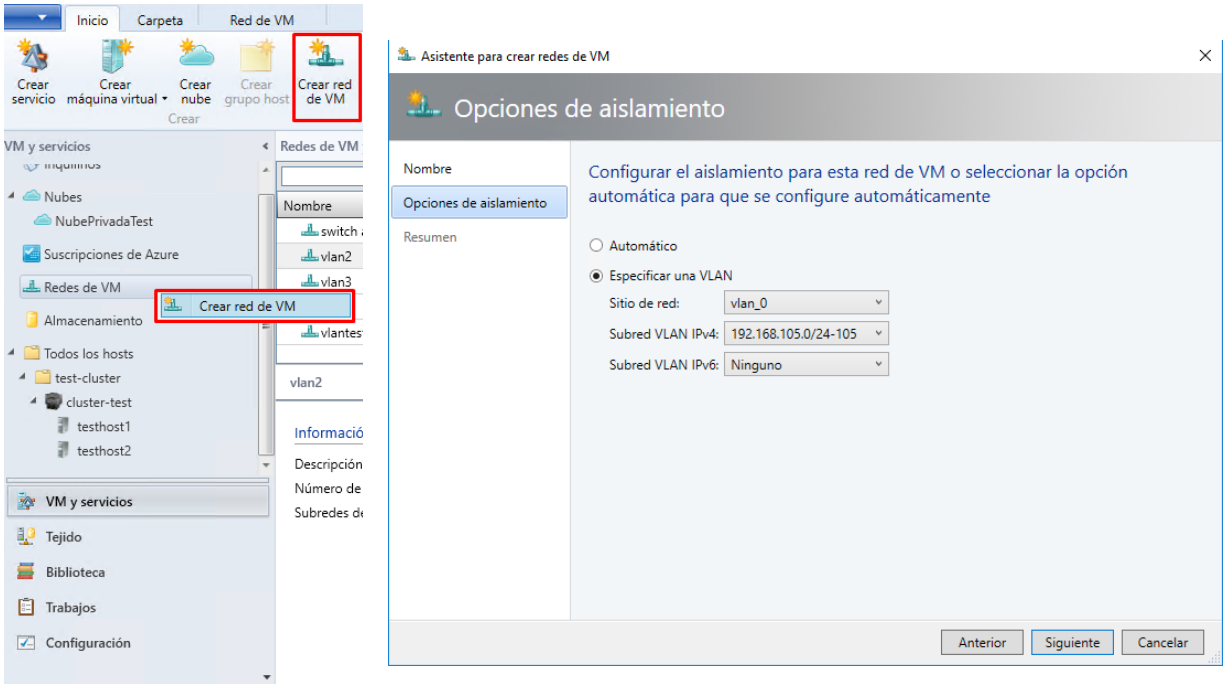


Figura 9.21: Creación de red de VM (izquierda) conectada a red lógica VLAN (derecha).

Nota

Si ya existe una red de VM conectada a una red lógica definida como *una red conectada*, como muestra la Figura 9.22, no se podrá conectar una nueva red de VM a esta.

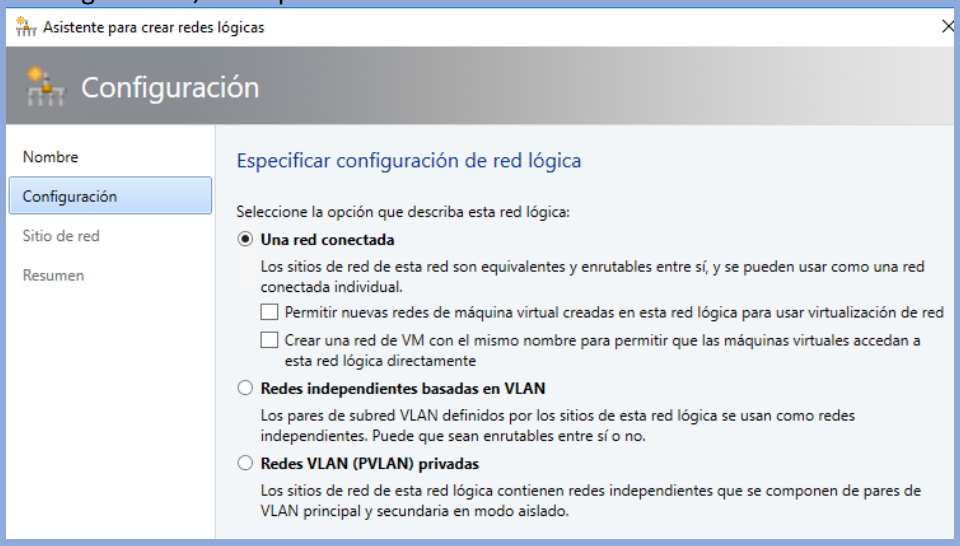


Figura 9.22: Red lógica con una red conectada.

Sin embargo, si se ha seleccionado una de las otras opciones para la red lógica, se pueden conectar tantas redes de VM como VLANs (con su correspondiente subred IP) existan. Para ello, por tanto, es necesario crear VLANs y subredes IP para cada red de VM que se desee conectar. Un ejemplo se muestra en la Figura 9.6. En esta se pueden ver varios sitios de red con varias VLANs y su correspondiente subred IP.

9.3.4 Almacenamiento

En este apartado se puede observar el almacenamiento de cada VM, la capacidad total del disco y la capacidad disponible, como se muestra en la Figura 9.23. Además, se puede acceder a las propiedades de la VM, que se explican en el apartado *Todos los hosts*.

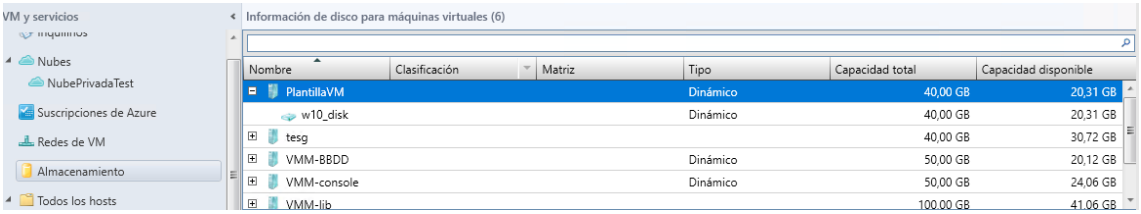


Figura 9.23: Almacenamiento de las VMs.

9.3.5 Todos los hosts

En este apartado, se pueden crear grupos host, igual que se hizo para agregar el clúster de *VMM* en la sección 8.1.3.3. Además, se pueden crear servicios y VMs y ver las redes de todos los hosts, como muestra la Figura 9.24.

Figura 9.24: Opciones en Todos los hosts.

9.3.6 Servicios

Para crear un nuevo servicio, lo primero que se solicita es si se quiere utilizar una plantilla de servicio, el nombre del servicio y el destino (se puede escoger una nube o un clúster específico) como se muestra en la Figura 9.25. Posteriormente, antes de poder implementar el servicio, se debe pulsar el icono *Clasificaciones* para ver si se puede ubicar el servicio en los hosts, o si hay algún error que solucionar (por falta de recursos o error en el servicio). Si todo está correcto, un ejemplo de lo que se observa aparece en la Figura 9.26.

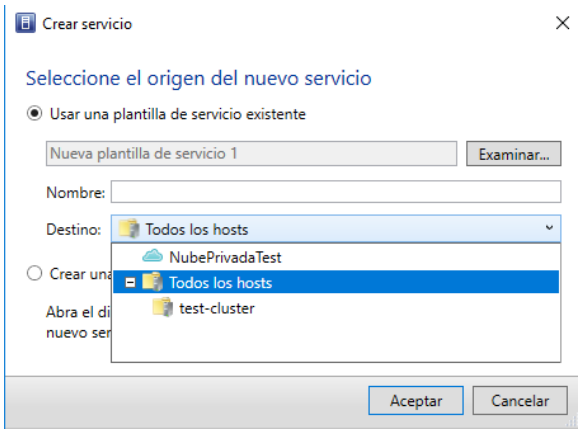


Figura 9.25: Selección de plantilla y ubicación.

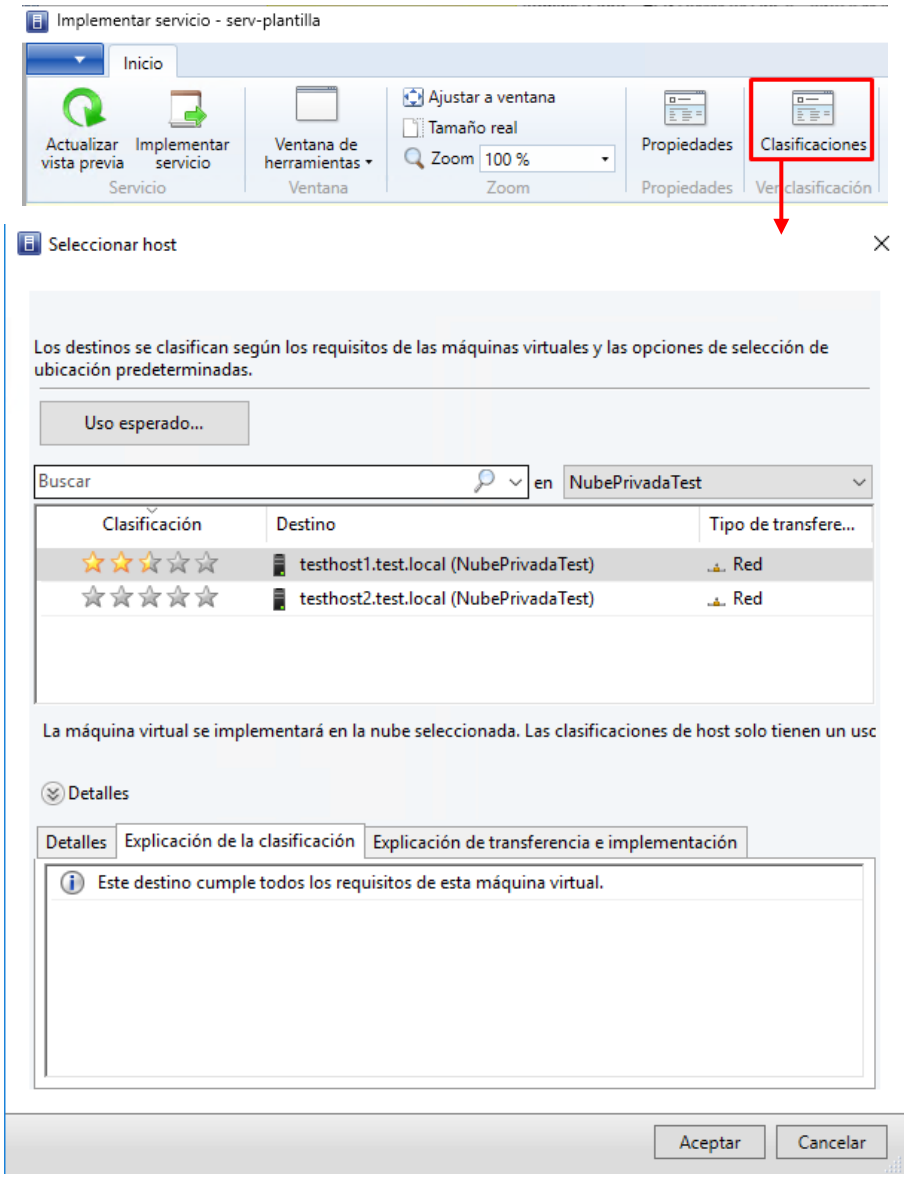


Figura 9.26: Selección de host para el servicio usando la opción *Clasificaciones*.

Utilizando, sin embargo, la opción *Actualizar vista previa, VMM* intenta ubicar el servicio automáticamente en alguno de los hosts.

Antes de implementar el servicio se pueden modificar el nombre de equipo y el nombre de las VMs que pertenezcan a este. Una vez terminado, el servicio se implementa utilizando el icono que aparece en la parte superior izquierda *Implementar servicio*. En caso de posponer la implementación, quedará guardada en *Biblioteca–Plantillas–Configuraciones de implementaciones*.

9.3.7 Máquinas virtuales

Para crear una nueva VM, igual que para crear un servicio, se debe especificar si utilizar una plantilla o no. Entre las opciones de plantilla se puede escoger utilizar una VM implementada en un host. Esta opción no elimina la VM como al utilizarla para crear una plantilla, sino que hace una clonación. De igual manera que al crear las plantillas de VM, el hardware no se puede modificar para este caso. Sin embargo, utilizando una plantilla o disco duro virtual sí es posible modificar el hardware. En cualquier caso, se debe seleccionar el destino de la VM para ubicarla en una nube, en alguno de los hosts o almacenarla en la biblioteca. Según la opción escogida, los siguientes pasos serán ligeramente distintos:

i. Si se escoge implementarlo en una nube, en el siguiente paso se debe especificar la nube en la que se debe implementar la VM.
ii. Si se escoge implementarlo en un host, se debe escoger en qué host ubicar la VM, las rutas de acceso para su configuración (en nuestro caso se ubican en el disco de clúster del NAS, explicado en la sección 8.3.1) y las redes de VM a la que va conectada, aunque se haya especificado ya en la configuración de hardware.
iii. Si se escoge almacenar la VM en la biblioteca, se debe especificar el servidor de biblioteca en el que se va a almacenar, y la ruta de acceso, es decir, en qué recurso compartido de la biblioteca se almacena.

Nota

Si la VM se crea desde plantilla, no se podrá crear si no se especifica una clave de producto en la configuración de S.O, tal y como muestra la Figura 9.27. Para evitarlo durante las pruebas, se puede crear un perfil de sistema operativo invitado con una clave de producto, y establecer ese perfil en esta configuración, como muestra la Figura 9.28.

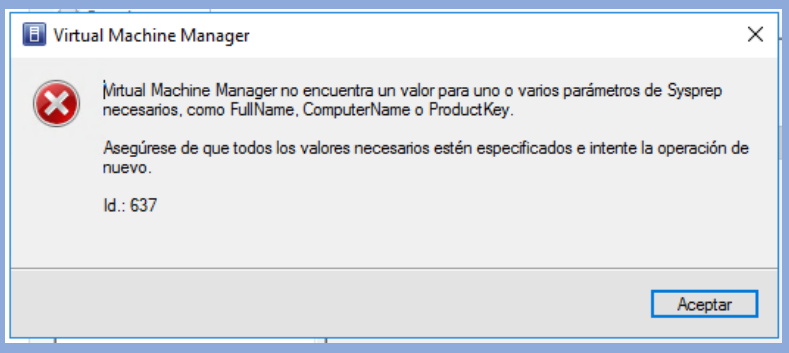


Figura 9.27: Error al crear una VM desde plantilla sin clave de producto.

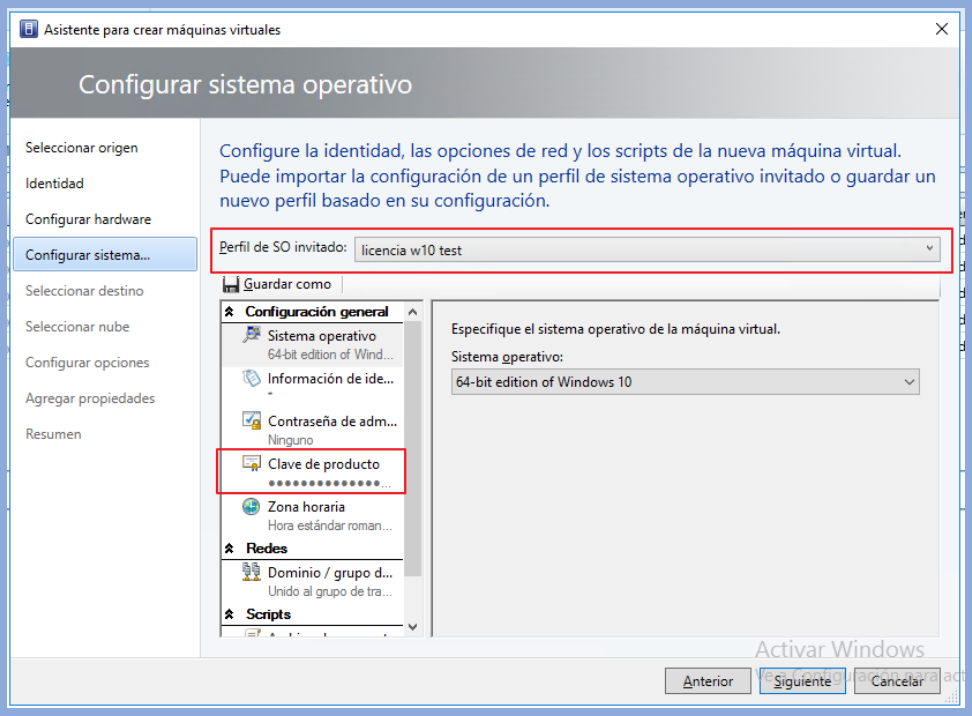


Figura 9.28: Utilización de Perfil de SO invitado en creación de VM.

Es importante destacar que, para poder modificar el nombre del disco duro virtual de una VM, sólo puede hacerse en el momento de crearla. Además, si se crea desde plantilla, ya sea plantilla de VM o desde disco, únicamente se puede modificar si se ubica en un host. Por este motivo es recomendable ubicarla en un host y posteriormente ubicarla en una nube. Este proceso se muestra a continuación. En la Figura 9.29 se pueden observar las opciones que aparecen al seleccionar un host como ubicación para modificar el nombre del disco, y en la Figura 9.30, la opción para ubicar la VM en una nube. Esta opción aparece en el apartado *General* de las propiedades de la VM.

Otra manera de modificar el nombre del disco de una VM es accediendo directamente al recurso de disco virtual almacenado en el NAS, modificar el nombre y posteriormente modificar sus propiedades para que utilice ese disco. Para ello, hay que acceder a la configuración de hardware de la VM, eliminar el disco que tiene con la opción *quitar*, como se ve en la Figura 9.31. Posteriormente, al añadir de nuevo un disco, se debe seleccionar el que ha sido modificado, como muestra la Figura 9.32.

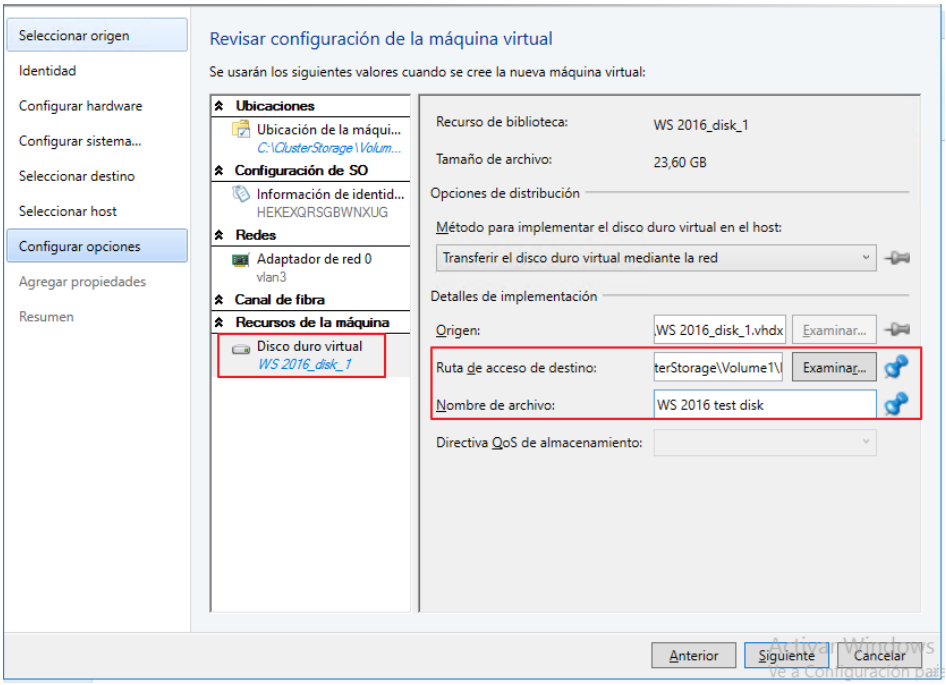


Figura 9.29: Cambio de nombre del disco de una VM al ubicarla en un host.

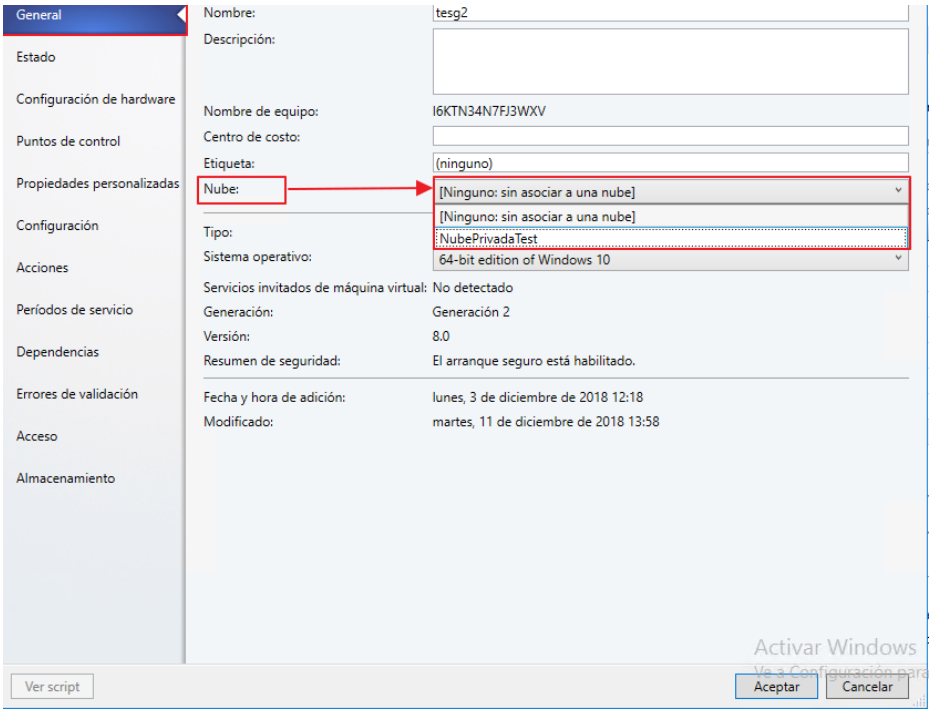


Figura 9.30: Ubicación de una VM en una nube.

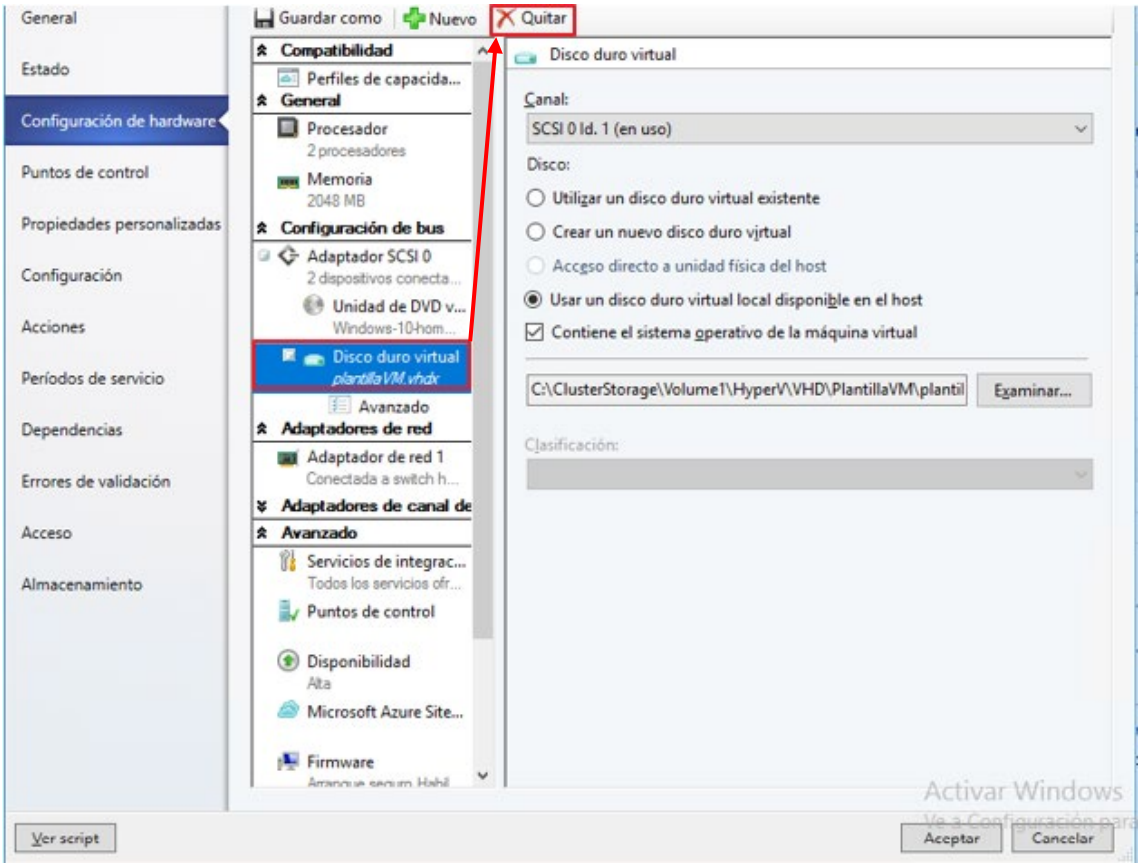


Figura 9.31: Eliminación del disco duro virtual asociado a la VM.

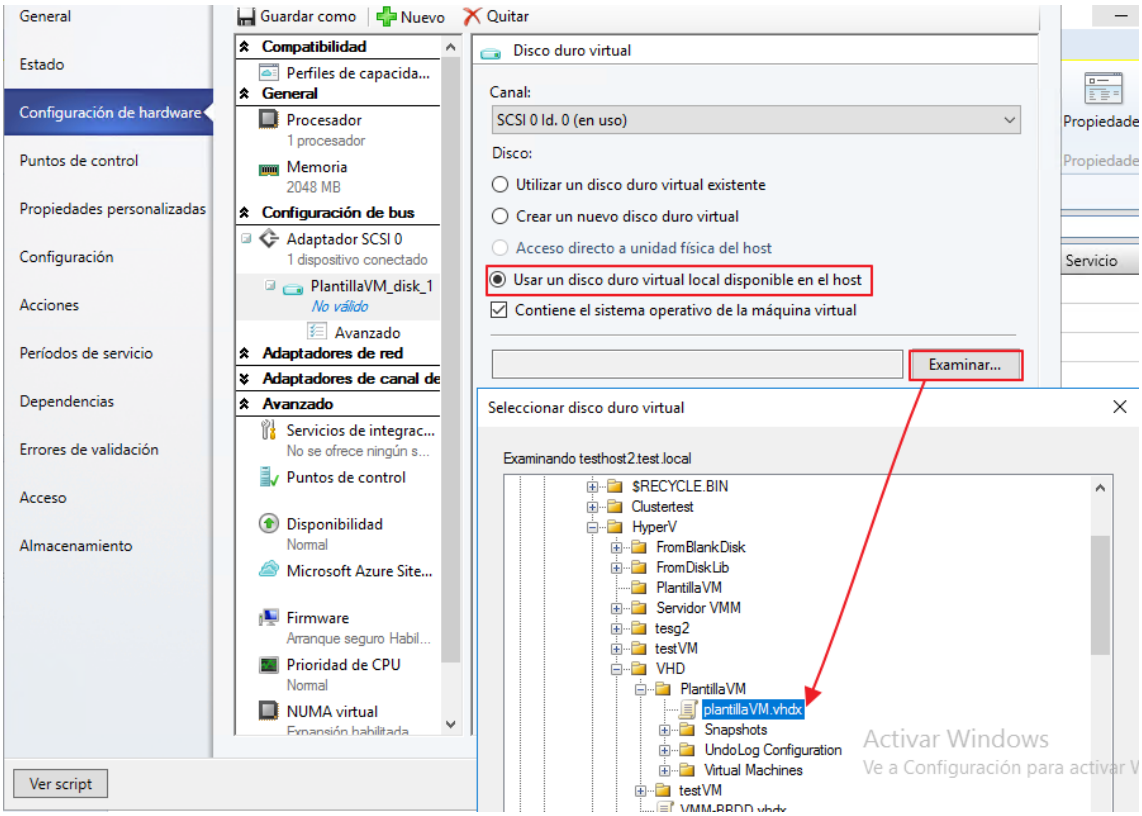


Figura 9.32: Utilizar el disco anteriormente renombrado.

Otro aspecto interesante que se puede hacer desde el apartado *Todos los hosts* es configurar el uso de los recursos de los hosts. Esto se puede hacer accediendo a las propiedades del grupo host que se desee modificar. La configuración puede ser heredada del grupo host primario (*Todos los hosts*) o se puede personalizar para cada grupo host. Modificando estas configuraciones se puede:

i. Modificar los recursos en reserva del host: estos recursos son reservados para el sistema operativo del host. En el momento de seleccionar la ubicación para las VMs, si para iniciarlas se requiere el uso de recursos en reserva del host, *VMM* notificará un error. En la Figura 9.33 se muestra un ejemplo de esta configuración.

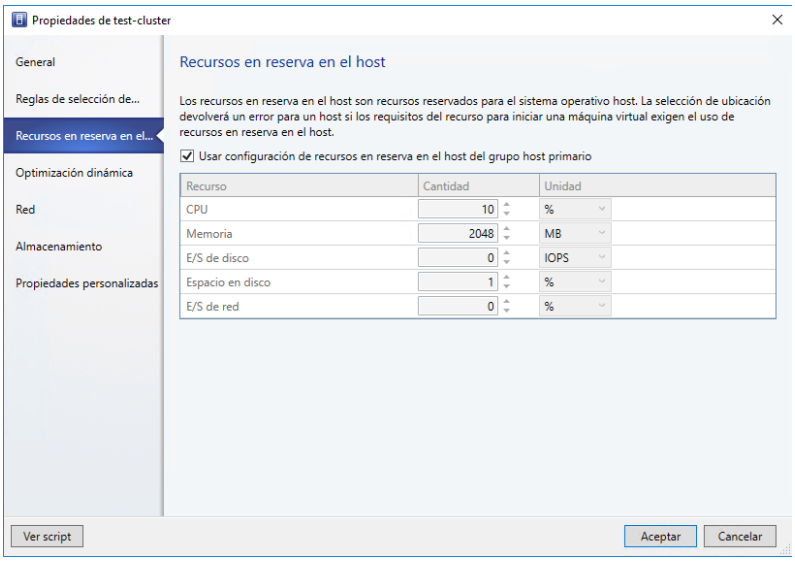


Figura 9.33: Opciones de recursos en reserva.

ii. Modificar las opciones de optimización dinámica: esta función equilibra la carga de la VM automáticamente en un clúster. Esta optimización se utiliza cuando los recursos disponibles están por debajo de un umbral, que se puede modificar. En el momento de seleccionar un host para migrar VMs, aparece un aviso en el caso de que el host seleccionado quede por debajo del umbral. Un ejemplo de la configuración se muestra en la Figura 9.34.

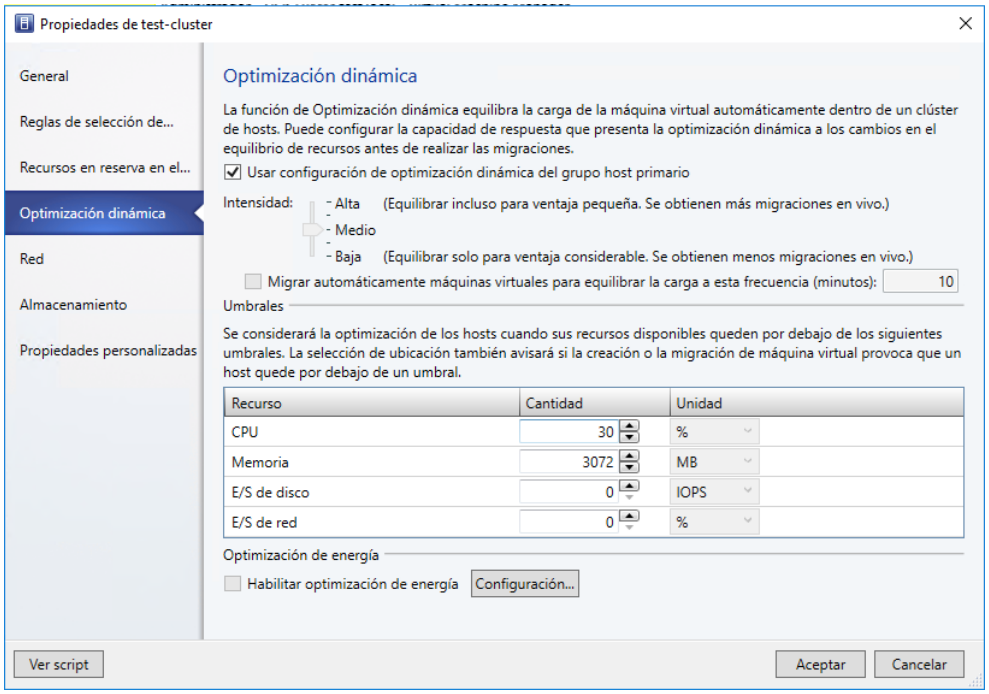


Figura 9.34: Opciones de optimización dinámica.

Por último, con permisos de administrador, se pueden ver todas las VMs que se hayan implementado en los hosts, obteniendo información:

i. De su estado.
ii. Del host en el que están implementadas.
iii. De la nube en caso de que se hayan implementado en una nube.
iv. Del propietario, del servicio del que puedan formar parte.
v. Del sistema operativo que tienen instaladas.

Además, se puede observar también al seleccionar alguna de las VMs información más específica, como se muestra en la parte inferior de la Figura 9.35. Destacar que estas columnas son las que se muestran por defecto, sin embargo, haciendo click derecho sobre los títulos, se puede modificar.

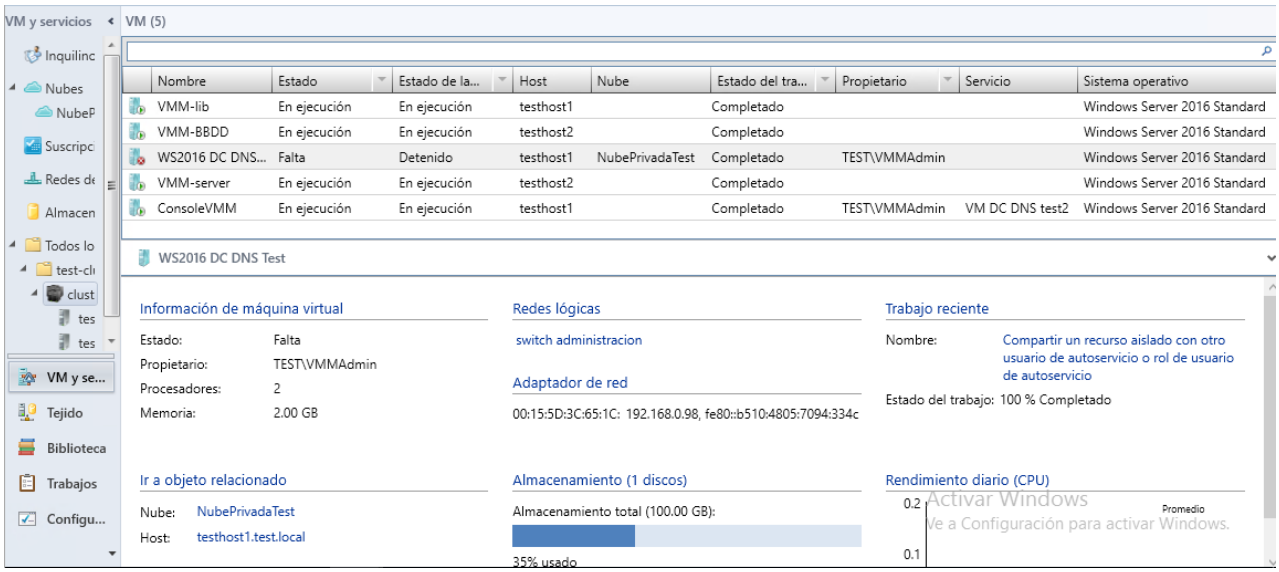


Figura 9.35: Información de las VMs en el clúster.

Sin embargo, al seleccionar una de las nubes, solo se pueden ver las VMs que formen parte de esta. Esto sirve principalmente para que, al crear nuevos usuarios, se les pueda ofrecer recursos sobre la nube, y así evitar tener que ofrecer recursos sobre los hosts directamente.

Haciendo click sobre estas VMs, se pueden realizar varias operaciones de igual manera que en Hyper-V o desde el administrador de clústeres, como se muestra en la Figura 9.36:

i. Apagar/Encender la VM.
ii. Migrar la VM a otro host.
iii. Almacenarla en biblioteca.
iv. Crear plantilla o clonarla.
v. Conectar a la VM.
vi. Eliminar la VM.
vii. Acceder a sus propiedades.

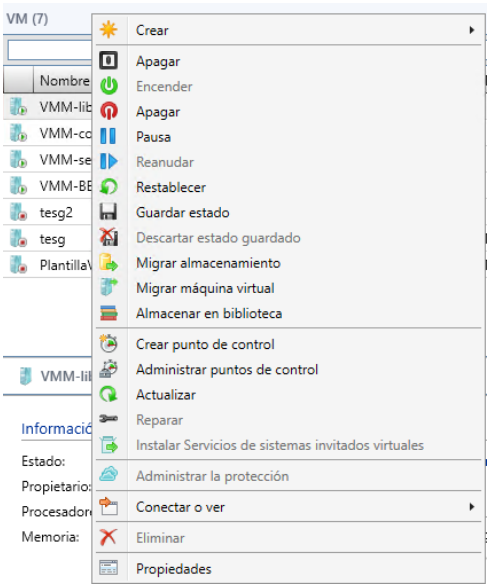


Figura 9.36: Opciones en las VMs.

Para finalizar con la sección de VM y Servicios, una manera interesante de observar de manera rápida el estado de cada apartado del *Cloud* es visualizar la información general. Pulsando este icono, y seleccionando el apartado que se desee observar, se obtiene información básica sobre las VMs, como muestra la Figura 9.37 (en la figura solo se muestra una parte de toda la información que aparece).

Figura 9.37: Información general de todos los hosts.

9.4 Configuración - Roles de usuario

Por último, y como punto importante, se explican los roles de usuario. Estos roles son los que permiten crear una jerarquía de permisos sobre el entorno *Cloud*, y así poder llevar un control sobre las acciones que cada usuario puede realizar. Además, gracias a estos roles, se puede ofrecer acceso a los clientes para que puedan reiniciar sus propios servidores en el *Cloud* sin peligro a que reinicien los de otros clientes.
Para crearlos, hay que acceder al apartado *Configuración*, y hacer click derecho sobre *Roles de usuario*. Mediante el asistente, lo primero que se debe indicar es el nombre del nuevo rol de usuario y una descripción. Seguidamente, se debe seleccionar el tipo de usuario que se desea crear. Los detalles de cada rol se muestran en la Tabla 9.2. El rol de administrador no se puede crear, este es el rol que existe por defecto, y al que pertenece el propietario de *VMM*.

Rol de usuario de *VMM*	Permisos	Detalles
Rol de administrador	Pueden realizar todas las acciones administrativas en todos los objetos que administra *VMM*.	Los administradores son los únicos que pueden agregar un servidor WSUS a *VMM* para habilitar las actualizaciones del tejido de *VMM* a través de *VMM*.
Administrador de tejido (administrador delegado)	Pueden realizar todas las tareas administrativas dentro de sus grupos host, nubes y servidores de biblioteca asignados.	Los administradores delegados no pueden modificar la configuración de *VMM*.
Administrador de sólo lectura	Pueden ver las propiedades, el estado y el estado del trabajo de los objetos de sus grupos host, nubes y servidores de biblioteca asignados, pero no pueden modificar los objetos.	El administrador de sólo lectura también puede ver las cuentas de ejecución que los administradores o los administradores delegados hayan especificado para el rol de usuario Administrador de sólo lectura.
Administrador de inquilinos	Pueden administrar usuarios de autoservicio y redes de VM.	Los administradores de inquilinos pueden crear, implementar y administrar sus propios servicios y máquinas virtuales a través de la consola *VMM* o un portal web[1]. También pueden especificar qué tareas pueden realizar los usuarios de autoservicio en sus máquinas virtuales y servicios. Los administradores de inquilinos pueden asignar cuotas a recursos computacionales y máquinas virtuales.
Administrador de aplicaciones (usuario de autoservicio)	Los miembros de este rol pueden crear, implementar y administrar sus propias máquinas virtuales y servicios.	Pueden administrar *VMM* mediante la consola *VMM*.

Tabla 9.2: información de los roles de usuario.

[1] Esta opción no está disponible desde la versión *VMM* 2012 R2.

Una vez escogido el tipo de rol de usuario que se desea crear, se deben especificar los miembros de este rol, que deben existir en Active Directory. Seguidamente, hay que seleccionar su ámbito, es decir, los objetos sobre los que los miembros del rol pueden realizar acciones. En este punto es donde empiezan a notarse las diferencias entre cada rol de usuario. Para los administradores de tejido y de lectura se pueden seleccionar tanto las nubes privadas como los hosts. Sin embargo, para los administradores de inquilinos y de autoservicio únicamente se pueden seleccionar nubes privadas, además de poder asignarles una cuota para limitar los recursos disponibles. Posteriormente, para los dos primeros roles, se debe asignar los servidores de biblioteca a los que tiene acceso, y las cuentas de ejecución disponibles. En cambio, para los dos últimos roles de usuario se deben especificar las redes de VM que puede utilizar, así como los recursos. Estos recursos son las VMs y los recursos de biblioteca a los que tienen acceso, sin conocer en que servidor de biblioteca o host de virtualización están ubicados. Por último, todavía para esos dos últimos roles se deben especificar los permisos globales para todas las nubes que pueden gestionar, y en caso de que sea necesario, permisos específicos para alguna de las nubes, como muestra la Figura 9.38.

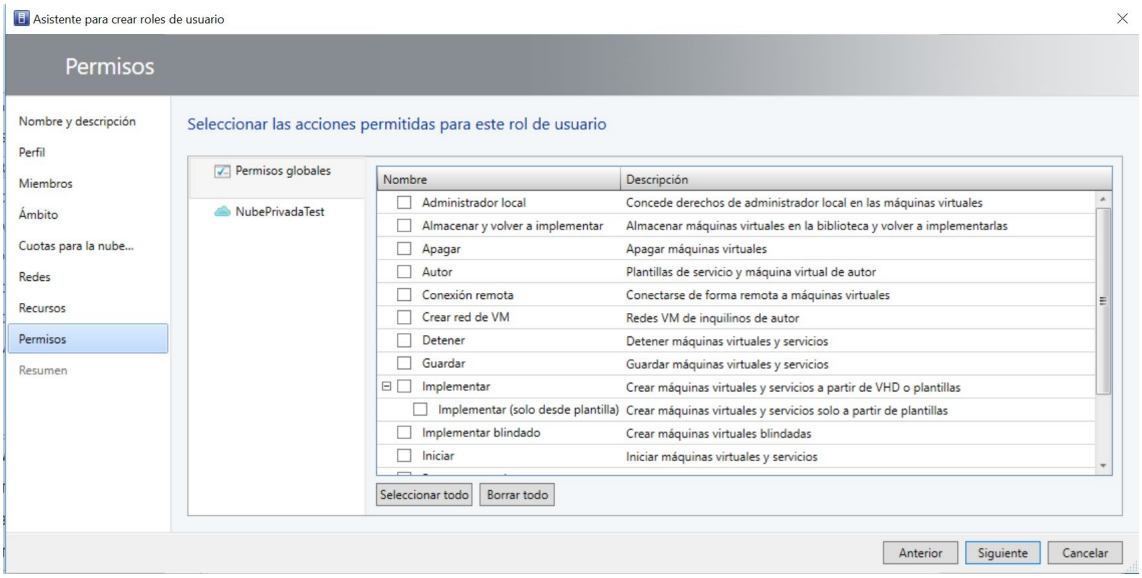


Figura 9.38: permisos de los roles de usuario de administrador de inquilinos y usuario de autoservicio.

Los permisos existentes y su función se detallan en la Tabla 9.3. Cabe destacar que los administradores de Inquilinos no tienen los permisos de *Recibir* ni *Compartir*, y cuentan con un permiso que se autodefine: *Crear red de VM.*

Permiso	Detalles
Autor	Crear plantillas y perfiles.
Punto de control	Crear, editar y eliminar puntos de control para sus propias máquinas virtuales y para restaurar una máquina virtual a un punto de control anterior. *VMM* no admite acciones de punto de control en los servicios.

Punto de control (solo restaurar)	Restaurar sus propias máquinas virtuales a un punto de control, pero no crear, editar ni eliminar puntos de control.
Implementar	Implementar máquinas virtuales y servicios desde plantillas y discos duros virtuales asignados a su rol. No pueden crear plantillas y perfiles.
Implementar (solo desde plantilla):	Implementar máquinas virtuales y servicios solo desde plantillas. Sin derechos de creación.
Administrador local	Administradores locales en sus propias máquinas virtuales. Se debe habilitar *Administrador local* en los roles de usuario con la acción *Implementar (desde plantilla)* para poder establecer la contraseña de administrador local durante la implementación.
Pausar y reanudar	Pausar y reanudar sus propias máquinas virtuales y servicios.
Recibir	Usar los recursos que compartan los miembros de otros roles de usuario de autoservicio.
Conexión remota	Conectarse a sus máquinas virtuales desde la consola *VMM* o App Controller.
Quitar/Guardar	Quitar o guardar sus máquinas virtuales.
Compartir	Compartir recursos de los que sean **propietarios** junto con otros roles de usuario de autoservicio. Entre los recursos que se pueden compartir se incluyen perfiles de hardware, perfiles de sistema operativo, perfiles de aplicación, perfiles de SQL Server, plantillas de máquina virtual, máquinas virtuales, plantillas de servicio y servicios. Para que un rol de usuario use los recursos, debe tener la acción ***Recibir***.
Iniciar/Detener	Iniciar y detener sus propias máquinas virtuales y servicios.
Almacenar y volver a implementar	Almacenar sus propias máquinas virtuales en la biblioteca *VMM* y volver a implementarlas. Las máquinas virtuales que están almacenadas en la biblioteca no cuentan para la cuota de máquina virtual del usuario. *VMM* no permite almacenar servicios.

Tabla 9.3: Permisos asignables a usuarios de autoservicio.

Para que los clientes puedan reiniciar sus propias VMs, es necesario crear un usuario para cada uno de ellos. Este usuario debe agregarse al rol de *usuario de autoservicio*.

Puede haber uno o más roles de autoservicio para ofrecer distintos permisos según el tipo de cliente. Por último, se le debe dar acceso a ese usuario a su/s VMs. Cabe destacar que a los usuarios del rol *Administrador de Inquilinos* también se les debe dar acceso a las VMs. Esto se hace o bien agregando las VMs a los recursos del rol, o bien de la siguiente manera:

i. Accediendo a las propiedades de la/s VM a la/s que se desee dar acceso, desde la sección *VM y servicios*, en el apartado de *Nubes.*

ii. Accediendo al apartado *acceso* de las propiedades, y agregar usuarios del dominio, como muestra la Figura 9.39.

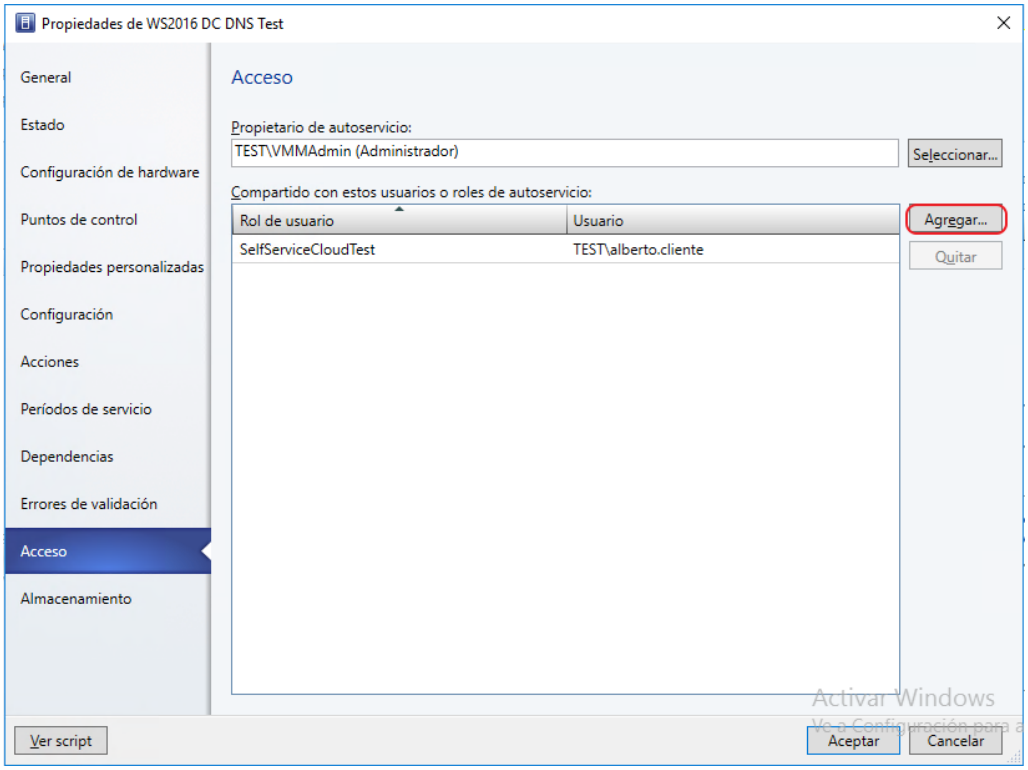


Figura 9.39: Agregar roles de autoservicio a VMs.

Para comprobar el funcionamiento, se han creado varios usuarios, entre ellos alberto.cliente, perteneciente al rol SelfServiceCloudTest mostrado en la figura anterior. Agregar el usuario es opcional. Si no se agrega, todos los miembros del rol SelfServiceCloudTest tienen acceso a la VM. Sin embargo, en el caso de los clientes, puede ser interesante tener un único rol de usuario para asignar los mismos permisos a ese rol, y filtrar los accesos a las VMs especificando un usuario. Si se quiere dar acceso a varios usuarios de un mismo cliente, también se pueden crear grupos en el controlador de dominio y filtrar el acceso por grupos en lugar de por usuarios. De esta manera, se evita tener que ofrecer el acceso usuario a usuario. Simplemente es necesario hacer que los usuarios de, por ejemplo, el cliente A, pertenezcan al grupo ClienteA. Así, en la Figura 9.39 se mostraría el grupo TEST\ClienteA en lugar de TEST\alberto.cliente.

Accediendo a *VMM* utilizando estos usuarios, únicamente se tiene acceso a los recursos a los que se le ha dado acceso, con los permisos ofrecidos. En este caso son:

i. Apagar VMs.
ii. Iniciar VMs.
iii. Pausar y reanudar VMs.
iv. Recibir.

Nota

La opción *Recibir* es necesaria si ese rol de usuario de autoservicio no es el *propietario de autoservicio* de esa VM.

En *VMM* son necesarias un mínimo de cuatro VMs que se encargan de ejecutar conjuntamente el servicio de *VMM*, además de las diferentes VMs implementadas para testing. No obstante, desde el punto de vista del cliente anteriormente nombrado, únicamente existe su VM. De igual manera, si no se le han asignado recursos de biblioteca, como por ejemplo plantillas de VM, no puede visualizarlas, como muestran las Figuras 9.40 y 9.41.

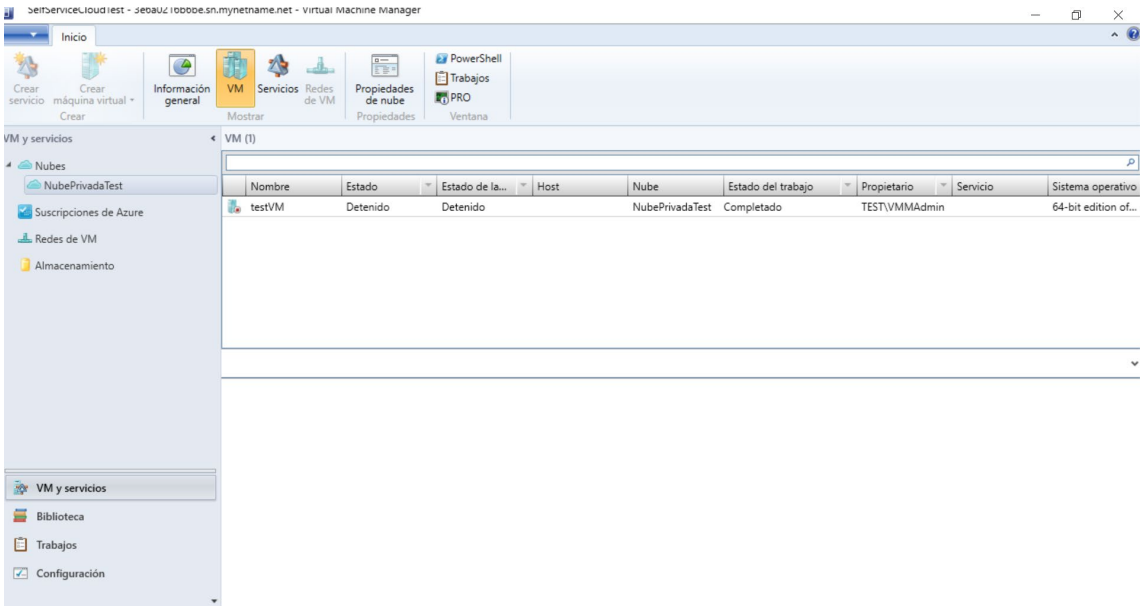


Figura 9.40: VMs accesibles desde el usuario alberto.cliente.

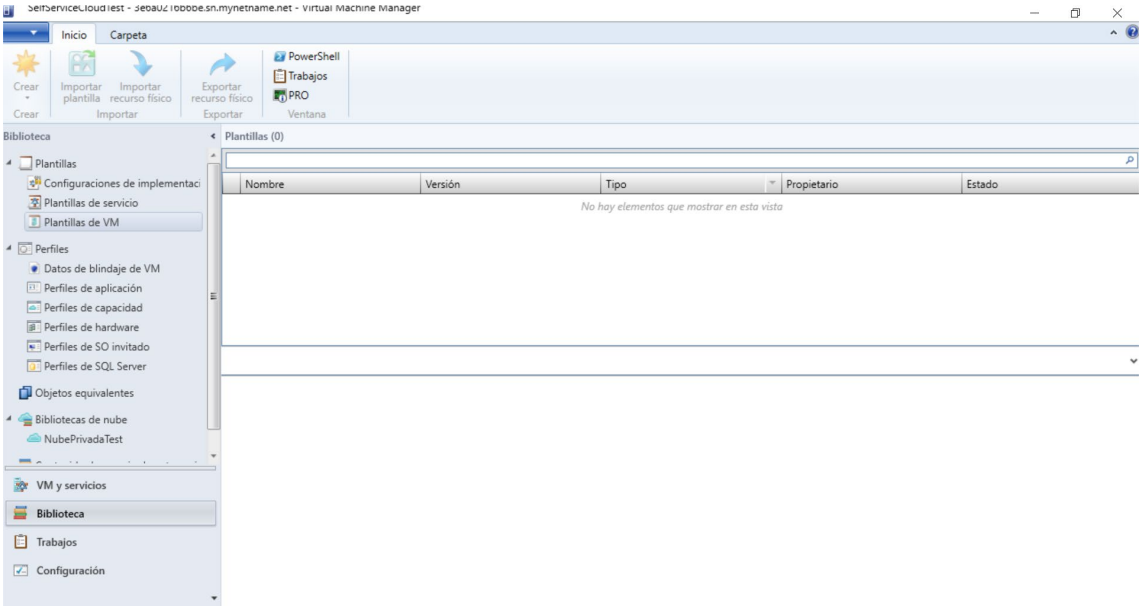


Figura 9.41: Recursos de biblioteca del usuario alberto.cliente.

De esta manera, si se intenta realizar cualquier acción distinta a las especificadas, por ejemplo, modificar opciones de hardware de la VM, se obtendrá un error similar al de la Figura 9.42*: el rol de usuario no tiene permisos suficientes.*

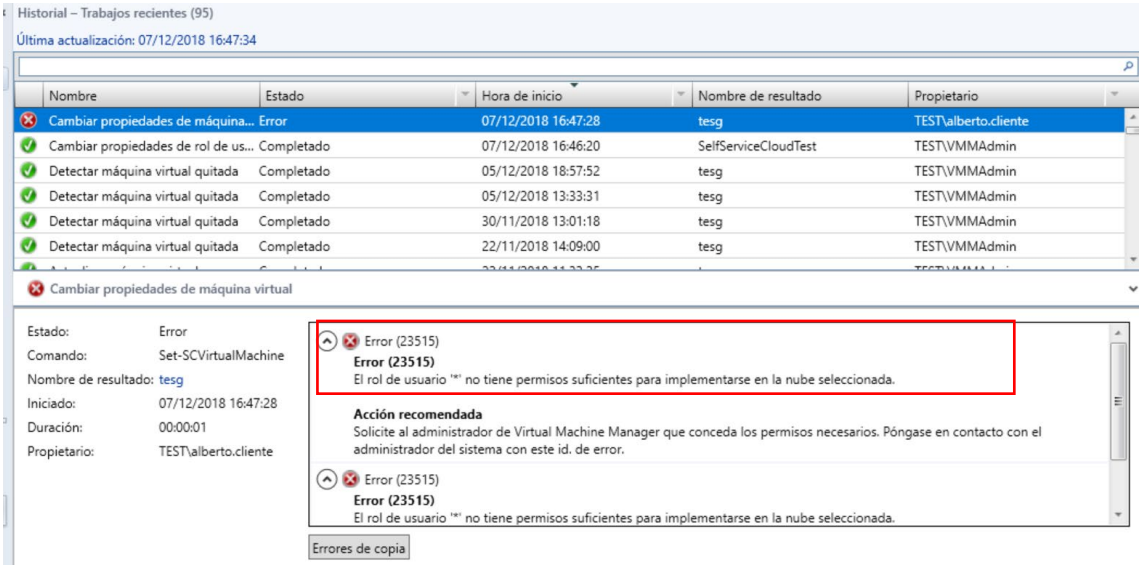


Figura 9.42: Error de permisos de rol de usuario.

Dado que Microsoft ha dejado de desarrollar una interfaz web de gestión *VMM* (no disponible desde la versión *VMM 2012 R2*), en un futuro proyecto se realizará una implementación propia a través de portal web seguro de escritorio remoto. De esta manera los clientes podrán tener acceso a *VMM* sin necesidad de ofrecer acceso remoto a la máquina de consola de *VMM.*

9.5 Pruebas de *VMM*

Este apartado pretende explicar los resultados de las pruebas realizadas con *VMM* con respecto a las pruebas mencionadas en la sección 4. Cabe destacar que la mayoría se detallan en los apartados anteriores, por lo que se intentará dar algún apunte extra, si necesario. Siguiendo el mismo orden tenemos:

i. **Pruebas de permisos de usuarios:** Los tipos de usuario y los permisos existentes se detallan en el apartado anterior. Una de las cosas que se ha echado en falta es la posibilidad de dar permisos específicos a un usuario en concreto en un rol, de la misma forma que tiene Windows. Por ejemplo, no es posible crear un único rol para los técnicos de ArdiCloud con permisos básicos para técnicos junior y senior. Esto se debe a que no hay ninguna opción para ofrecer permisos únicamente a ciertos miembros de ese rol, como modificar los discos de VM, apagar las máquinas o eliminarlas.

ii. **Pruebas de VMs:** En este apartado se incluyen las pruebas de plantillas, que, igual que para los permisos de usuarios, se detallan en su mayoría en los apartados anteriores. Destacar que para la creación de VM desde plantillas es necesario especificar una clave de producto del S.O. Esto impide crear, por ejemplo, una VM con Windows desde plantilla para realizar alguna prueba si en el momento de crearla no se especifica la licencia para activar Windows. Es por este motivo por el cual se ha creado un perfil de SO invitado para poder almacenar una licencia para la realización de las pruebas. Destacar que *VMM* cumple con los objetivos marcados sobre VMs, y permite desplegar una o varias máquinas de manera sencilla gracias a las plantillas de VM y servicios.

iii. **Pruebas de redes virtuales:** Se han alcanzado todos los objetivos marcados respecto a la securización de red, tanto a nivel infraestructura datacenter como a nivel de redes privadas de clientes. Dichos objetivos se han conseguido a través de herramientas exclusivas de *VMM* como redes lógicas y redes VM. Como opción de mejora y evolución del proyecto (a través de un segundo) quedaría el desarrollo de otras características de *VMM* como los conmutadores lógicos, los perfiles de puerto y los servicios de red.

iv. **Pruebas de copias de seguridad y de fallos del sistema:** Actualmente se realizan las copias de seguridad de la infraestructura a través de la herramienta complementaria a *SCVMM* llamada *SCDPM* (System Center Data Protection Manager). Queda pendiente la posibilidad de implementar una segunda capa de seguridad a través de *SCVMM* y Azure Site Recovery, que se propone como punto de desarrollar en un posible segundo proyecto.

v. **Pruebas de reporting/logging:** *VMM* permite tener una traza de todos los trabajos realizados, obteniendo información de quién ha lanzado el trabajo, en qué momento, sobre qué recurso y cuál es su estado (en ejecución, completado con éxito o con erro), tal y como muestra la Figura 9.43. También permite tener

información detallada de toda la infraestructura mediante la *Información General* que ofrece en todas sus secciones (redes, nubes, máquinas virtuales, almacenamiento,…).

Sin embargo, no existe la posibilidad de monitorizar el estado de las VMs de manera proactiva (por ejemplo, una VM que se esté quedando sin espacio en disco). Actualmente se utiliza la herramienta de monitorización Zabbix (basado en código abierto y muy similar a Nagios[1]), aunque en el futuro se analizará la herramienta Microsoft System Center Operations Manager (*SCOM*) y se valorará su posible implemetación en sustitución.

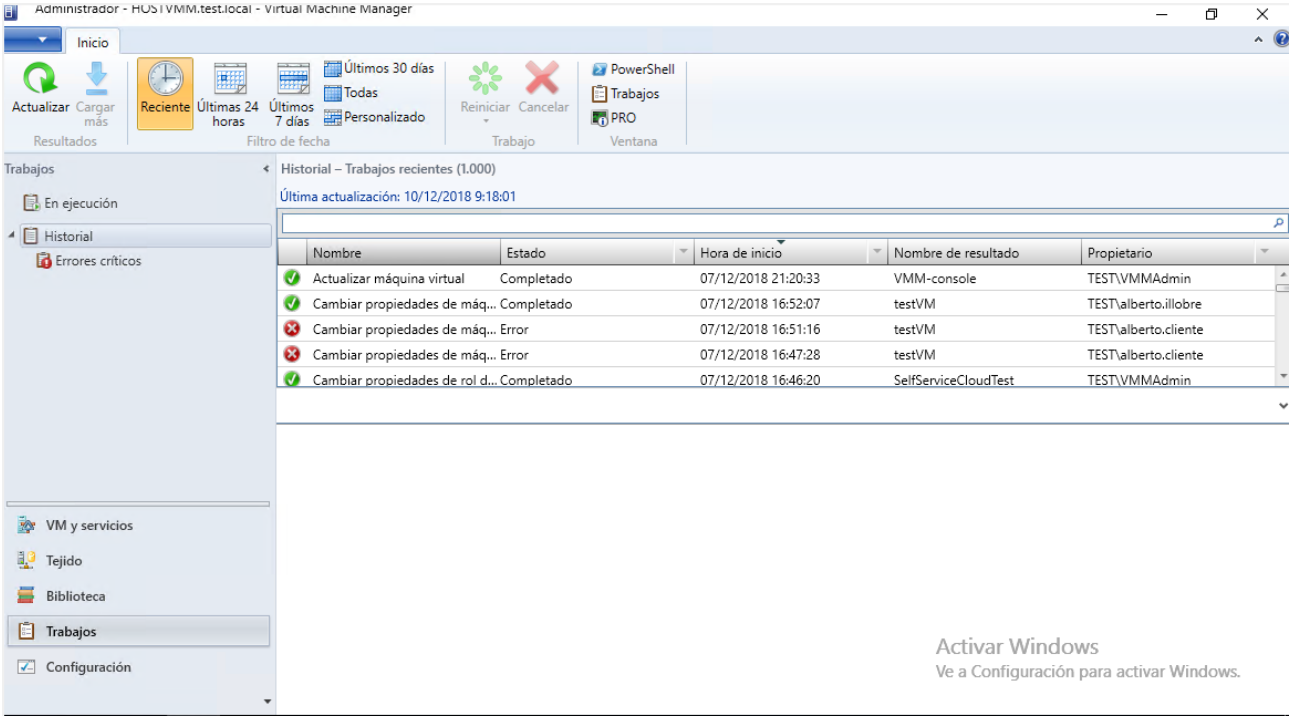


Figura 9.43: Sección de Trabajos de *VMM*.

[1] Software de monitorización de equipos y servicios de red.

9.6 Comparación con el entorno actual

Seguidamente, se comentan los puntos principales por los cuales este sistema pretende sustituir al sistema actual, ya que agiliza y simplifica las tareas de los técnicos.

Como se ha visto en la preparación del entorno, para poder crear VMs de manera rápida sin *VMM*, es necesario tener una ya creada y conservar el recurso de disco duro virtual. Este proceso es igual utilizando *VMM*. Sin embargo, *VMM* permite tener todas las plantillas organizadas en un recurso compartido, además de poder especificar una descripción de estas y así utilizarlas de forma sencilla. Sin la librería de *VMM*, es necesario saber exactamente donde está ubicado ese disco que se quiere utilizar como plantilla, además de tener que conocer exactamente qué sistema y/o aplicaciones contiene. El añadido de poder utilizar scripts en el despliegue de VMs, agiliza todavía más el trabajo, ya que un proceso que actualmente se realiza en unas horas, se puede hacer en unos minutos y esperar a que el proceso termine sin la necesidad de hacer configuraciones intermedias.

Como también se ha visto, utilizando *VMM* se puede saber de forma rápida qué redes están siendo utilizadas y por quién. Utilizando las herramientas actuales, habría que observar una a una las VMs para poder obtener esa información. *VMM* también permite una configuración de red utilizando virtualización (como VLANs). Esta configuración no puede hacerse directamente desde Hyper-V, que únicamente permite la conexión de sus teams o tarjeas físicas a un conmutador virtual al que se conectan posteriormente las VMs.

Además, obtenemos una información general sobre el almacenamiento de las VMs, para poder avisar a los clientes en caso que se estén quedado sin espacio de almacenamiento. Se puede observar también el rendimiento de la CPU de cada VM, para poder así monitorizar su estado. Sin utilizar *VMM* esto se debe hacer de forma manual, accediendo a la propia VM y utilizando la herramienta de Windows: *monitor de rendimiento*. Con esta herramienta se pueden activar contadores de rendimiento durante varios días/semanas, y así obtener la información necesaria. Esto implica que a veces, no se puede ser proactivo, es decir, hasta que no se activan esos monitores de rendimiento y se visualizan los resultados, no se puede saber el estado de la VM. Con las mejoras futuras de *Operations Manager*, se podrá obtener todavía más información.

Uno de los puntos probablemente más importantes son los permisos de usuario. Sin utilizar *VMM* hay que acceder directamente a los hosts de virtualización con un usuario de administrador para poder realizar cualquier modificación de las propiedades de las VMs. Este hecho implica que no se pueden limitar los accesos a los diferentes recursos según el usuario, lo que obliga a restringir mucho el acceso e imposibilita ofrecer acceso a sus propias VMs a los clientes. Con *VMM* y los accesos basados en usuario, todos los técnicos que necesiten realizar alguna gestión en el *Cloud* podrán acceder cada uno con los permisos que tenga asignados. El hecho de que existan permisos también hace que

un técnico inexperto no pueda provocar un desastre en el *Cloud*, como por ejemplo eliminar, por error, una VM de un cliente o de administración. En cualquier caso, si esto ocurriese, gracias a la sección de *Trabajos*, se podrá saber exactamente qué ha pasado en todo momento,y por quién. Por lo tanto se podrá solucionar el problema de forma rápida y también aprender de los errores.

Por otra parte, también permitirá dar acceso a los clientes a sus propios recursos, e incluso actuar sobre ellos o modificarlos si fuera necesario.

Desarrollo del proyecto: Implementación en el entorno real

Por razones organizativas de la empresa, la implementación de VMM en la infraestructura actual se ha planificado para el mes de agosto de 2019. Se aprovechará para hacer cambios estructurales como la reorganización y ampliación de recursos hardware. Por otra parte, se realizarán cambios en el diseño de la red, lo que podría implicar pequeños cortes en el servicio los cuales son menos críticos en esas fechas.

De igual manera que durante la fase de pruebas, es necesario preparar el entorno para instalar el sistema VMM. En el caso del entorno real, la parte física está preparada, por lo que únicamente es necesario crear las VMs del sistema. Los pasos son similares que los seguidos durante la fase de testing y se explican en la sección 10.1. Para grandes infraestructuras es totalmente necesaria la implementación de sistemas de management redundantes, ya que un fallo en los mismos imposibilitaría la gestión de manera manual dada la complejidad de estos. En entornos pequeños (como es el caso de ArdiCloud, que actualmente dispone de 10 hosts, 2 cabinas de discos con conectividad fibre channel) una caída de cualquiera de los elementos de management (consola, servidor *VMM* o base de datos *VMM*) supondría que la gestión durante el tiempo de restablecimiento debería realizarse de forma manual.

Teniendo en cuenta el alto crecimiento de la infraestructura en los últimos 2 años (casi se ha triplicado la capacidad) y previendo el de los próximos, se está considerando la opción de implementar ya de inicio un sistema completamente redundante, mediante la instalación de un segundo servidor de administración de *VMM* y un segundo servidor SQL VMM (en configuración de clúster). La VM de librería no se debería modificar demasiado por lo que con las copias de seguridad de máquinas virtuales se podría restablecer. Esto implicaría la pérdida de las plantillas creadas posteriormente a la última copia realizada (se realizan copias diarias de toda la infraestructura). Además, un fallo de ésta únicamente impediría la utilización de plantillas. Por último, la VM de consola se utiliza únicamente para poder acceder a *VMM*, que se encuentra en las VMs de Servidor de administración *VMM*, con su configuración guardada en la base de datos por lo que, de nuevo, es suficiente con restablecer la última copia realizada.

En vista de la situación actual y de los cambios previstos, y teniendo en cuenta que la instalación y configuración de *VMM* puede realizarse con el servicio *Cloud* en ejecución, no debería presentarse ningún obstáculo siempre y cuando dichos cambios se realicen siguiendo el procedimiento. En cualquier caso, se informará a los clientes sobre el intervalo de tiempo de actuación por si fueran necesarias acciones que pudieran provocar bajadas en el rendimiento (p.ej. movimiento masivo de VMs entre hosts,

reorganización de cableado que requiera la entrada en funcionamiento de los sistemas redundantes…).

La configuración inicial de las redes lógicas VMM se realizará a través del proceso automático de creación, tal y como se ha visto en la sección 9.1. De esta manera las VMs no verán alterada su conectividad de red. Asimismo, las nuevas redes lógicas y redes de VMs creadas para mejorar la seguridad en el *Cloud*, se crearán sin asignarlas a ninguna VM inicialmente. Una vez creadas, se modificará de forma ordenada la configuración de las VMs del entorno hasta que todas queden con la conectividad deseada. Esto puede parecer un proceso lento, pero en la realidad se podrá aplicar de forma relativamente rápida y mucho más controlada.

En cualquier caso, se ha hecho una planificación de la configuración que se realizará en VMM. Esta planificación incluye la creación de roles de usuario, plantillas de VM y servicios (y sus perfiles relacionados), y el diseño de red inicial (conmutadores virtuales, redes lógicas, redes de VM de clientes y grupos de direcciones IP). Esta configuración se realizará como muestra la Figura 10.1 y se explica a continuación:

iii. **Roles de usuario:**
   a. *Administradores globales*: a este rol, creado automáticamente al instalar VMM y sin restricciones sobre el entorno gestionado por *VMM*, se le agregarán los miembros de mayor cargo.
   b. *Rol de Administrador de Tejido o Delegado:* se creará un rol de este tipo para que los técnicos más experimentados puedan realizar gestiones sobre todo el entorno *Cloud* (a excepción de realizar modificaciones sobre la configuración de *VMM*).
   c. *Rol de Administrador de sólo Lectura: s*e creará un rol de este tipo para que técnicos de otros departamentos puedan visualizar el estado de todo el entorno (tanto hosts como VMs de administración y de clientes), sin la posibilidad de realizar modificaciones.
   d. *Rol de Administrador de Inquilinos: s*e creará un rol de este tipo para los técnicos junior. Se les asignará permisos sobre la(s) nube(s) privada(s), para que puedan realizar gestiones sobre las máquinas de los clientes, pero no sobre los hosts o VMs de administración.
   e. *Rol de usuario de Autoservicio: s*e creará un rol de este tipo para cada cliente (con permisos básicos). Dicho rol se asignará a la nube privada correspondiente (de esa manera cada cliente podrá gestionar únicamente sus VMs).

i. **Plantillas de VM y servicios**: ArdiTEC es un proveedor de servidores C*loud* "gestionados". El target de clientes es muy específico, teniendo éstos unas necesidades muy específicas tanto a nivel de producto (ERP SAGE, soluciones Enterprise de Microsoft…) como a nivel de servicio (clientes sin departamento IT, o con uno de pequeñas dimensiones). Esto implica que la mayoría de las

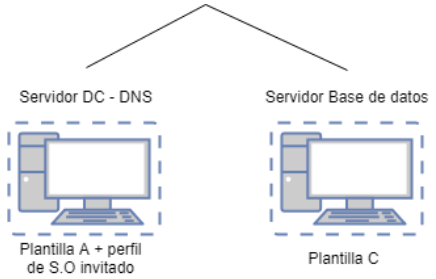
instalaciones (80-90%) se pueden desplegar a través de cuatro *plantillas de VM* y un *perfil de S.O invitado* con las siguientes características:

a. Plantillas de VM:
    1. Plantilla A con Windows Server 2016 Datacenter (licenciamiento SPLA[1]).
    2. Plantilla B con Windows Server 2016 Datacenter y Office 365 Empresa E3 (licenciamiento CSP[2]).
    3. Plantilla C con Windows Server 2016 Datacenter y SQL Server 2017 Standard (licenciamiento SPLA).
    4. Plantilla D con Windows Server 2016 Datacenter, SQL Server 2017 Standard y Office 365 Empresa E3.

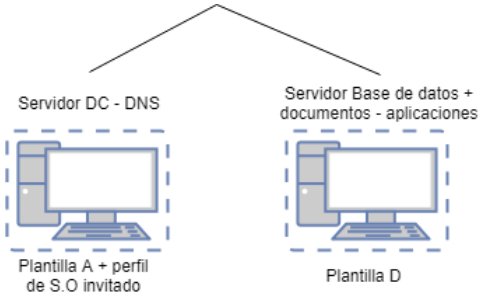
b. Perfil de S.O invitado para la instalación de los roles Active Directory-DNS.

Con esta definición de plantillas, serán necesarios tres *servicios de VMM* para el despliegue automático de las siguientes posibles configuraciones de servidores *Cloud*:

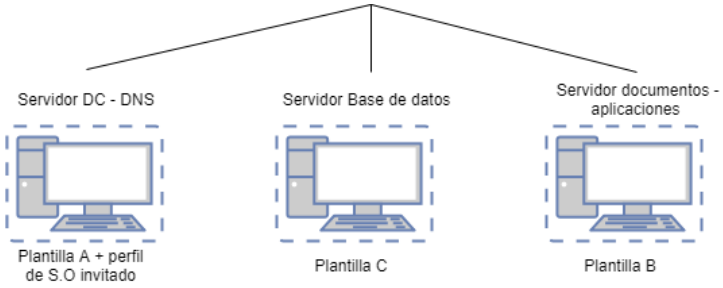
a. Cliente pequeño con datos en local:



b. Cliente pequeño con datos en el *Cloud*:



c. Cliente mediano con datos en el *Cloud*:



[1] **Microsoft Services Provider License Agreement. Se alquilan las licencias mensualmente.**
[2] Microsoft Cloud Solution Provider. Se paga por suscripción mensualmente.

d. Para clientes grandes la configuración de VMs se realiza a medida, por lo que no tiene sentido guardar una configuración de servicio para este caso.

iii. **Diseño de red inicial:** La configuración de redes debe ser una representación del entorno real. Así pues, y teniendo en cuenta las modificaciones que se realizarán en la infraestructura de red, se crearán las siguientes redes virtuales:

a. Red lógica basada en VLAN para la infraestructura con 3 VLANs
   1. VLAN 1: Red de dispositivos BackUp.
   2. VLAN 2: Red de clúster (comunicación entre los nodos).
   3. VLAN 3: Red de administración. Para esta red se creará una red de VM, que se asignará a las VMs de administración.

b. Red lógica de tipo una red conectada con virtualización de red para los servidores de clientes. Para esta red lógica se creará un grupo de direcciones IP para cada cliente.
   1. Por cada cliente se creará una Red de VM con su respectivo grupo de direcciones IP (el cual es subgrupo o grupo completo del grupo creado en la red lógica).

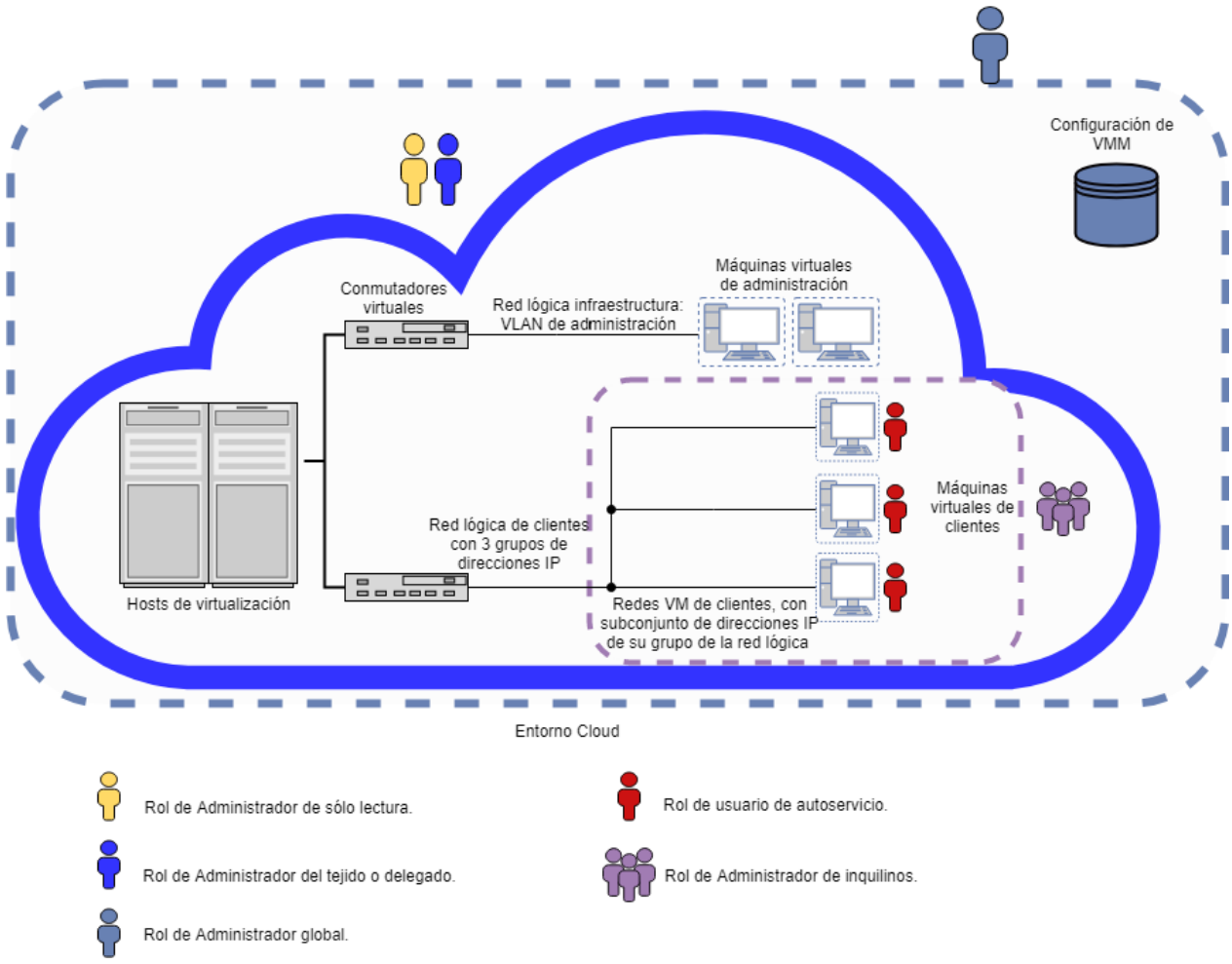


Figura 10.1: Configuración de usuarios y redes.

10.1 Puesta en marcha del sistema redundante

Como se ha comentado, lo ideal es contar con un sistema completamente redundante. Para ello, son necesarios dos nodos de administración de *VMM* y dos nodos de SQL, con la configuración apropiada para ofrecer alta disponibilidad. Antes de instalar los dos nodos de administración de *VMM*, es necesario instalar SQL y configurar los grupos de disponibilidad AlwaysOn en dos VMs. Estas máquinas deben estar en un clúster de conmutación por error independiente. Es necesario un segundo clúster para los nodos de administración de *VMM*. La configuración necesaria para realizar la instalación del sistema completamente redundante se explica esquemáticamente a continuación. La mayoría de los pasos son similares a los seguidos durante la instalación en el entorno de testeo.

i. **Base de datos de *VMM* (SQL):**
   a. Crear el clúster para los dos nodos de SQL y añadirlos.
   b. Instalar SQL Server en ambos nodos.
   c. Configurar las bases de datos VMM con grupos de disponibilidad AlwaysOn en ambos nodos.
      c.1 Detener el servicio de SQL de la instancia creada en la instalación.
      c.2 Activar la opción de la instancia *AlwaysOn Availability Groups.*
      c.3 Reiniciar el servicio.
      c.4 Crear base de datos temporal y habilitar la opción de *Back Up*.
      c.5 Crear nuevo *Grupo de Disponibilidad* y especificar la base de datos de *Back Up* con con las opciones de *Replicas* que se deseen.
      c.6 Crear un *Listener* para el grupo de disponibilidad y añadirlo a la lista de traducciones del servidor DNS.

ii. **Biblioteca:**
   a. Crear un clúster de conmutación por error para ambos nodos de biblioteca.
   b. Seleccionar *Configurar rol* en el *Administrador de clústeres de conmutación por error*.
   c. Seleccionar el rol *Servidor de archivos* en el *Asistente para alta disponibilidad.*
   d. Especificar el nombre e IP del clúster en *Punto de acceso de cliente.*
   e. Especificar el almacenamiento compartido que se desea usar.
      e.1 *Agregar un recurso compartido de archivos* seleccionando el servidor de archivos en *Administración de clústeres de conmutación por error.*
      e.2 En el asistente seleccionar el perfil *Recurso compartido SMB – Rápido.*

e.3 Conceder acceso completo a las cuentas del sistema, administradores y a la cuenta de administración de *VMM.*

iii. **Servidor de administración de *VMM:***

a. Crear el clúster para ambos nodos de servidor de *VMM.*
b. Crear el contenedor para las claves distribuidas, de igual forma que para la instalación del entorno de test.
c. Instalar los componentes pre-requisitos de *VMM* en ambos nodos, de igual forma que para el entorno de test.
d. Instalar *VMM* en el primer nodo.
   d.1 Al estar en clúster debería aparecer un aviso al seleccionar *Servidor de administración VMM* para realizar la instalación de alta disponibilidad.
   d.2 Especificar el *Listener* de SQL en la configuración de base de datos.
   d.3 Especificar el clúster de *VMM*.
e. Instalar *VMM* en el segundo nodo.
   e.1 Al estar en clúster e instalado en un primer nodo, aparece un aviso para agregar este nodo a la instalación de alta disponibilidad.
f. Agregar la biblioteca.
   f.1 Agregar el clúster de biblioteca.

10.2 Futuras líneas de trabajo

En apartados anteriores se han mencionado varias posibles mejoras, sobretodo respecto a la gestión de la infraestructura completa (hosts, VMs, monitorización…) y a la recuperación frente a desastres. Estas se detallan a continuación:

i. Ofrecer acceso a los clientes a través de un portal web de escritorio remoto en lugar de mediante la consola de *VMM.*
ii. Mejorar la monitorización de *VMM* para poder sustituir el software Zabbix a través de la herramienta Microsoft System Center Operations Manager (SCOM). Esto se debe a que *VMM* ofrece la posibilidad de observar el estado de las VMs, pero no mediante notificaciones.
iii. Utilización de scripts en el despliegue de VMs. Este punto es útil para entornos grandes en el que se deban desplegar varias VMs a diario.
iv. Integración con Azure Site Recovery para así poder ofrecer una mayor disponibilidad a los clientes.

10.3 Otras características

Durante la realización de las pruebas se ha priorizado aquellas características necesarias para ArdiCloud. A diferencia del apartado anterior, las siguientes características no se aplicarán a corto plazo, pero existe la posibilidad de estudiarlas:

i. **Tejido:**
   a. Redes:
      1. *Conmutadores lógicos*: se utilizan para aplicar configuraciones específicas a través de los *perfiles de puerto, clasificaciones de puerto* y *servicios de red*.
      2. *Plantillas de VIP*: una plantilla de IP virtual (VIP) contiene las opciones de configuración de carga equilibrada para un tipo específico de tráfico de red.
   b. Almacenamiento:
      1. Clasificaciones y grupos: clasificaciones de almacenamiento para agrupar el almacenamiento según las características compartidas, el rendimiento frecuente y la disponibilidad.
      2. Servidores de archivos: Las cargas de trabajo virtualizadas de System Center - Virtual Machine Manager (VMM) requieren recursos de almacenamiento para satisfacer los requisitos de capacidad y rendimiento.
      3. Directivas QoS: directivas de calidad de servicio

Conclusiones

Gestionar un entorno *Cloud* creciente sin la ayuda de herramientas de gestión puede ser tedioso. La simplificación y centralización de las tareas de gestión ha hecho necesario el desarrollo de este proyecto, cuyos objetivos se establecen en la sección 2.

El desarrollo de este proyecto se planificó de manera que las fases han quedado bien diferenciadas siguiendo los objetivos establecidos. Así, se ha preparado un entorno de testeo completo para poder realizar todas las pruebas pertinentes, y comprobar el funcionamiento de la herramienta *SCVMM* antes de implementarla en el entorno *Cloud* de producción. La realización de estas pruebas ha sido importante debido principalmente al coste de la herramienta. Como añadido, las pruebas también han servido para proveer a los técnicos de una documentación de las funcionalidades necesarias, y así agilizar el proceso de aprendizaje. Por este motivo, se ha redactado la documentación de manera que sirva como guía para el uso del sistema *SCVMM.*

En conclusión, los objetivos establecidos para este proyecto se han cumplido, a excepción de la implementación en el entorno real, que se ha planificado en profundidad. La formación a los usuarios finales se hará a medida que se utilice el sistema. Además, el entorno de testeo se sigue utilizando para seguir realizando pruebas. En consecuencia, se podrán continuar estudiando en mayor profundidad las funcionalidades con las que cuenta *VMM* y así poder agilizar y simplificar las tareas de los técnicos en la mayor medida posible.

Finalmente, las competencias técnicas requeridas para completar el proyecto se detallan en el Apéndice A.

Apéndice A: Competencias técnicas de Ingeniería de Computadores

CEC2.1: Analizar, evaluar, seleccionar y configurar plataformas hardware para el desarrollo y ejecución de aplicaciones y servicios informáticos.

Esta competencia ha sido cubierta en profundidad dado que este proyecto se basa en el análisis y evaluación de la herramienta *SCVMM* para la gestión de un servicio informático, en concreto un servicio *Cloud*.

CEC2.2: Programar considerando la arquitectura hardware, tanto en ensamblador como en alto nivel.

Una de las características, a pesar de que no se ha profundizado en exceso, es la preparación de scripts para agilizar el proceso del despliegue de aplicaciones y servicios durante la creación de nuevas VMs en el sistema.

Todas las acciones realizadas en VMM tienen un equivalente en Powershell. Así pues, en cada apartado tenemos la posibilidad de ver el comando equivalente, lo que nos permite automatizar configuraciones complejas en caso de que sea necesario.

CEC4.1: Diseñar, desplegar, administrar y gestionar redes de computadores.

Durante el proyecto se han diseñado y desplegado redes para el entorno *Cloud*, por lo que esta competencia se ha cubierto en profundidad.

CEC4.2: Demostrar comprensión, aplicar y gestionar la garantía y la seguridad de los sistemas informáticos.

Se han gestionado sistemas redundantes: servidores en cluster, con redundancia de red, redundancia de alimentación, redundancia de datos a través de SANs con volúmenes RAID y controladoras redundantes…

Pese a que no se ha incluido en el proyecto, también se han realizado pruebas de copias de seguridad con las herramientas utilizadas en producción (Hyperoo y Microsoft Data Protection Manager).

Bibliografía

1. *¿Qué son los Hipervisores?* [Online]. Available: http://www.datakeeper.es/?p=716.
2. Admin, "*Cloud* computing: origen y evolución de la nube," *cisga*, 30-Jun-2017. [Online]. Available: https://www.cisga.es/conoces-origen-del-*Cloud*-computing-nube-informatica/.
3. "Breve historia del *Cloud* Computing," *MakeSoft Technologies*, 07-Oct-2016. [Online]. Available: https://www.makesoft.es/es/breve-historia-del-*Cloud*-computing/.
4. "Computación en la nube," *Wikipedia*, 24-Sep-2018. [Online]. Available: https://es.wikipedia.org/wiki/Computación_en_la_nube.
5. "Hipervisor," *Wikipedia*, 18-Sep-2018. [Online]. Available: https://es.wikipedia.org/wiki/Hipervisor.
6. "Internet World Stats," *Senegal Internet Usage and Telecommunications Reports*. [Online]. Available: https://www.internetworldstats.com/.
7. Lichtigstein, "VMware vs. Microsoft Hyper-v: is VMware Still Far Ahead?," *Loom Systems*. [Online]. Available: https://www.loomsystems.com/blog/vmware-vs.-microsoft-hyper-v-is-vmware-still-far-ahead.
8. "Microsoft Hyper-V vs. VMware: How far is VMware Still Ahead?," *Rob's Blog - Microsoft Technology Evangelist*, 23-Aug-2018. [Online]. Available: https://www.netwatch.me/2018/08/22/microsoft-hyper-v-vs-vmware-how-far-is-vmware-still-ahead/.
9. "Modelos de servicio en la nube | Tipos de *Cloud* computing | AWS," *Amazon*. [Online]. Available: https://aws.amazon.com/es/types-of-*Cloud*-computing/.
10. "Qué es virtualización - Definición | Microsoft Azure," *A beginner's guide | Microsoft Azure*. [Online]. Available: https://azure.microsoft.com/es-es/overview/what-is-virtualization/?cdn=disable&OCID=AID719820_SEM_&gclid=Cj0KCQjwof3cBRD9ARIsAP8x70OlPNIVE6iHsHc9JDftzj2SwfLj6dC2Fpm4noh94ok5MOKspZE0Hd0aAvOHEALw_wcB&dclid=CJzTucLTwd0CFZS3GwodiusMTA.
11. Scooley, "Introducción a Hyper-V en Windows 10," *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/about/.
12. Shortpatti, "Virtualización," *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/windows-server/virtualization/virtualization.
13. "What is VMware? - Definition from WhatIs.com," *SearchVMware*. [Online]. Available: https://searchvmware.techtarget.com/definition/VMware.
14. "What is a Hypervisor? - Definition from Techopedia," *Techopedia.com*. [Online]. Available: https://www.techopedia.com/definition/4790/hypervisor.
15. "What is a Private *Cloud* - Definition | Microsoft Azure," *A beginner's guide | Microsoft Azure*. [Online]. Available: https://azure.microsoft.com/en-us/overview/what-is-a-private-*Cloud*/.

16. “¿Qué es la informática en la nube? Guía para principiantes | Microsoft Azure,” *A beginner's guide | Microsoft Azure*. [Online]. Available: https://azure.microsoft.com/es-es/overview/what-is-*Cloud*-computing/.
17. “*Cómo comprar System Center*,” *Software Asset Management – Microsoft SAM*. [Online]. Available: https://www.microsoft.com/es-es/*Cloud*-platform/system-center-pricing#ft1.
18. “*How to buy System Center*,” *Software Asset Management – Microsoft SAM*. [Online]. Available: https://www.microsoft.com/en-cy/*Cloud*-platform/system-center-pricing.
19. *Vinzeo*. [Online]. Available: https://www.vinzeo.com/
20. “*Productos informáticos y tecnológicos* - Servicios para necesidades interempresariales - Ingram Micro,” *Ingram Micro Inc.* [Online]. Available: https://es-new.ingrammicro.com/.
21. “Download and install the Windows ADK,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/windows-hardware/get-started/adk-install.
22. “Descargar SQL Server Management Studio (SSMS) - SQL Server,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017.
23. “Configurar la biblioteca en el tejido de proceso de *VMM*,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/system-center/vmm/manage-library-server?view=sc-vmm-1807.
24. “Configurar redes para hosts y clústeres de Hyper-V en el tejido de *VMM*,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/system-center/vmm/hyper-v-network?view=sc-vmm-1807.
25. “Instalar la consola de *VMM*,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/es-es/system-center/vmm/install-console?view=sc-vmm-1807.
26. “Plan *VMM* installation,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/en-us/system-center/vmm/plan-install?view=sc-vmm-1807.
27. “Nagios,” [Online]. Available: https://www.ecured.cu/Nagios.